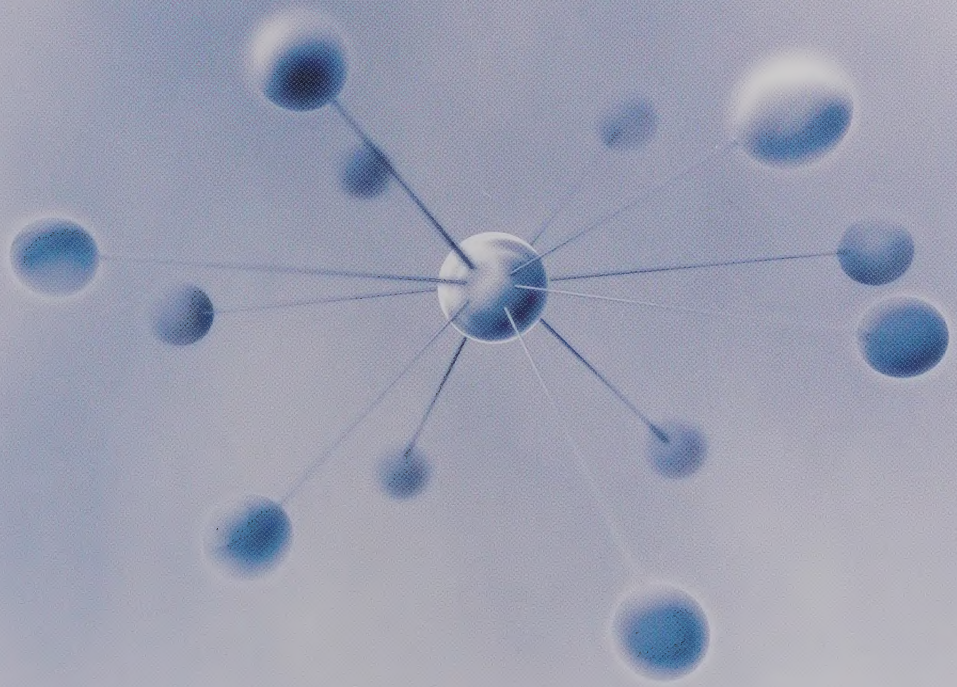
Agilent Network Troubleshooting Center

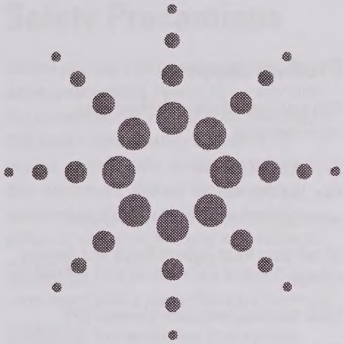


Getting Started Guide

Agilent Technologies

Digitized by the Internet Archive
in 2025

https://archive.org/details/manualsplus_09051



J6781A
Agilent Network Troubleshooting Center

Getting Started Guide

Agilent Technologies

Notices

Copyright © 2003 Agilent Technologies, Inc. All rights reserved.

No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Agilent Technologies, Inc. as governed by United States and international copyright laws.

Manual Part Number

5971-6321

Edition

First Edition, January 2003

Software version 1.0

Printed in Singapore

Printing History

New editions of this guide are issued to reflect extensive changes made to the software. Revisions may be issued, between editions, to correct errors in the manual. There may not be a new edition issued in conjunction with every software release.

Trademarks

Microsoft ® is a U.S. registered trademark of Microsoft Corporation.

Windows ® and MS Windows ® are U.S. registered trademarks of Microsoft Corporation.

Agilent Network Troubleshooting Center acknowledges several trademarks and copyrights - please see book appendix.

Product Support

Call your local Agilent Technologies representative, or:

Tel: 1-800-452-4844
Fax: 303-754-4802
www,agilent.com/find/techsupport

or call your local Agilent Sales and Service Office.

Web: www.agilent.com/comms/XPI

Agilent Technologies, Inc.
1900 Garden of the Gods Road
Colorado Springs, CO 80907-3483

Documentation Warranty

The material contained in this document is subject to change without notice. Agilent Technologies makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Agilent Technologies shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

A copy of the specific warranty terms applicable to your product and replacement parts can be obtained from your local Sales and Service Office.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Certification

Agilent Technologies certifies that this product met its published specifications at the time of shipment from the factory. Agilent Technologies further certifies that its calibration measurements are traceable to the United States National Institute of Standards and Technology (formerly National Bureau of Standards), to the extent allowed by that organization's calibration facility, and to the calibration facilities of other International Standards Organization members.

Restricted Rights Legend

If Software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Agilent Technologies' standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Safety Precautions

Before you use this instrument, read these safety precautions. Failure to comply with the precautions or with specific warnings in this book violates safety standards of design, manufacture, and intended use of this instrument. Agilent Technologies assumes no liability for the customer's failure to comply with these requirements.

WARNING This product is a Safety Class I instrument with a protective earth terminal.

WARNING For protection from electric shock hazard, power cord ground must not be defeated.

Operating Restrictions

The following general safety precautions must be observed during all phases of operation, service, and repair of this instrument. Failure to comply with these precautions with specific warnings in this manual violate safety standards of design, manufacture, and intended use of this instrument.

Grounding

To minimize shock hazard, the instrument chassis and cabinet must be connected to an electrical ground. The instrument is equipped with a three-conductor AC power cable compatible with an approved three-contact electrical outlet. The power jack and mating plug of the power cord must meet International Electrotechnical Commission (IEC) safety standards.

Environment

Do not operate the instrument in the presence of flammable gases or fumes. Operation of any electrical instrument in such an environment constitutes a definite safety hazard.

Service and Adjustment

Dangerous voltages exist within this instrument. Service and adjustment of this instrument is to be performed only by trained service personnel.

Do not replace components with the power cable connected.[1] Dangerous voltages may be present even when the power cable is disconnected.

[1] Note this exception: You can exchange Line Interface Modules with the power cable connected and power applied.

Do not perform internal servicing or adjustment unless another person, capable of rendering first aid and resuscitation is present.

Hazardous Material

Should the LCD be damaged, the liquid crystal material can leak. Avoid all contact with this material, especially swallowing. Use soap and water to thoroughly wash all skin and clothing contaminated with the liquid crystal material.

Unauthorized Service

The installation of substitute parts or the installation of any instrument modification not authorized by Agilent Technologies is specifically forbidden. The performance of such unauthorized service can negate the instrument warranty or any maintenance agreements.

Return the instrument to an Agilent Sales and Service Office for authorized service and repair.

Electric Shock Hazard

Do not remove the system covers. To avoid electric shock, use only the supplied power cords and connect only to properly grounded (3-pin) wall outlets.

Explosion Hazard

Do not operate in the presence of flammable gases.

Fire Hazard

For continued protection against fire hazard replace only with fuse of same type and rating.

Cleaning

To clean the product, use a damp cloth moistened with a mild solution of soap and water. *Do not* use harsh chemicals. *Do not* let water get into the product.

Product Damage

Do not use this product when the product shows visible damage, fails to perform, has been stored in unfavorable conditions, or has been subject to severe transport stresses.

Whenever this product has become damaged or wet, make the product inoperative and secure it against any unintended operation. Contact your nearest Agilent Sales office for assistance.

Instruction book symbol - the product will be marked with this symbol when it is necessary for the user to refer to the instruction book in order to protect against damage.

A product marked with this symbol indicates it is a laser product. When necessary, this symbol will be included in the instruction book for the user to refer to in order to protect against personal injury and/or correct product handling.

Indicates potential for electrical shock.

This is an Installation Category II product.

This is a Pollution Degree 2 product.

This product is designed for indoor use only.

FCC Part 68 Disclaimer

This equipment must not be connected to the telephone network unless it is connected through protective circuitry that is registered pursuant to Part 68 of the Federal Communications Commission rules.

AGILENT TECHNOLOGIES, INC. SOFTWARE LICENSE TERMS

ATTENTION: USE OF THE SOFTWARE IS SUBJECT TO THE LICENSE TERMS SET FORTH BELOW.

IF YOU DO NOT AGREE TO THESE LICENSE TERMS, DO NOT INSTALL THE SOFTWARE AND YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS NOTICE, INSTALLING OR OTHERWISE USING THE SOFTWARE INDICATES YOUR ACCEPTANCE OF THESE TERMS.

AGILENT SOFTWARE LICENSE TERMS

The following License Terms govern your use of the Software unless you have a separate written agreement with Agilent, in which case, that written agreement will control and take precedence.

Software. "Software" means one or more computer programs in object code format, whether stand-alone or bundled with other products, and related documentation.

License Grant. Agilent grants you a non-exclusive license to use one copy of the Software for internal purposes in accordance with these license terms and the documentation provided with the Software. Such documentation may include license terms provided by Agilent's third party suppliers, which will apply to the use of the Software and take precedence over these license terms. In the absence of documentation specifying the applicable license, you may use one copy of the Software on one machine or instrument. If the software is licensed for concurrent or network use, you may not allow more than the maximum number of authorized users to access and use the software concurrently.

License Restrictions. You may make copies or adaptations of the Software only for archival purposes or only when copying or adaptation is an essential step in the authorized use of the Software. You must reproduce all copyright notices in the original Software on all permitted copies or adaptations. You may not copy the Software onto any public or distributed network.

Upgrades. This license does not entitle you to receive upgrades, updates or technical support. Such services may be purchased separately.

Ownership. The Software is owned and copyrighted by Agilent or its third party suppliers. Agilent and its third party suppliers retain all right, title and interest in the Software. Agilent's third party suppliers may protect their rights in the Software in the event of any violation of these License Terms.

No Disassembly. You may not disassemble or otherwise modify the Software without written authorization from Agilent, except as permitted by law. Upon request, you will provide Agilent with reasonably detailed information regarding any permitted disassembly or modification.

High Risk Activities. The Software is not specifically designed, manufactured or intended for use in the planning, construction, maintenance or direct operation of a nuclear facility, nor for use in on line control or fail safe operation of aircraft navigation, control or communication systems, weapon systems or direct life support systems.

Transfer. You may transfer the license granted to you here provided that you deliver all copies of the Software to the transferee along with these License Terms. The transferee must accept these License Terms as a condition to any transfer. Your license to use the Software will terminate upon transfer.

Termination. Agilent may terminate your license upon notice for breach of these License Terms. Upon termination, you must immediately destroy all copies of the Software.

Export Requirements. If you export, re-export or import Software, technology or technical data licensed hereunder, you assume responsibility for complying with applicable laws and regulations and for obtaining required export and import authorizations. Agilent may terminate this license immediately if you are in violation of any applicable laws or regulations.

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data – Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

Documentation Map

This Getting Started Guide provides information on how to set up and use Agilent's Network Troubleshooting Center.

There are other documents that you will need to refer to. They are:

Network Troubleshooting Center and Network Analyzer Software Setup Guide

J6800A Network Analyzer Hardware Setup Guide

J6802A Distributed Network Analyzer MX Hardware Setup Guide

J6801A Distributed Network Analyzer Hardware Setup Guide

J6805A Distributed Network Analyzer ME Hardware Setup Guide

Network Analyzer Getting Started Guide

Contents

1 Introduction

Introduction to the Agilent Network Troubleshooting Center (NTC) 10

Network Troubleshooting Center Architecture and Components 11

- Agilent NTC Console 13
- Agilent NTC Server 13
- Agents 13

Network Troubleshooting Center Deployment 15

Features Overview 18

- Agent Management 19
- Data Display 20
- Global Configuration 26

2 Getting Started

Setup Process Overview 28

Deploy Agents 29

- Deploying Agilent Network Analyzer Agents 29
- Deploying Other SNMP MIB2, RMON, and RMON2 Agents 32

Install the Network Troubleshooting Center 34

Start the Network Troubleshooting Center and Begin Testing 37

- Starting and Stopping the NTC Server 37
- Starting the NTC Console 39
- Adding, Discovering, and Managing Agents 42
- Viewing Collected MIB-II, RMON, and RMON2 Data 54
- Running a Remote Troubleshooting Session on an Agilent Agent 57

Other Useful Features to Note 60

- Event Viewer 60
- Global Configuration 60
- NTC Console Customization 60

3 Licensing, Performance, and Other Operational Information

Licensing 64

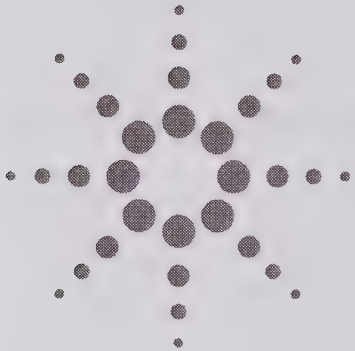
Purchasing an NTC Product Allowing More Physical Interfaces 64
Data Sources, Logical Interfaces, and Physical Interfaces 65
Licensing and Performance Requirements 66
Licensed Physical Interfaces and Starting a Remote Session 67

Integrating with HP OpenView Network Node Manager 69

A Appendix: RMON/RMON2 Fundamentals

B Appendix: Copyright Notices

Copyright Notices and Acknowledgements 82



1 Introduction

Introduction to the Agilent Network Troubleshooting Center (NTC) 10
Network Troubleshooting Center Architecture and Components 11
Network Troubleshooting Center Deployment 15
Features Overview 18

Introduction to the Agilent Network Troubleshooting Center (NTC)

The J6781A Agilent Network Troubleshooting Center (NTC) is a powerful software tool used to monitor and troubleshoot local area and wide area networks (LANs and WANs). Agilent's NTC is used by network test personnel who need to combine the advantages of dispatched and centralized network testing to streamline the troubleshooting process. NTC is a key component in Agilent's centralized network troubleshooting solution.

Agilent's NTC allows you to do the following:

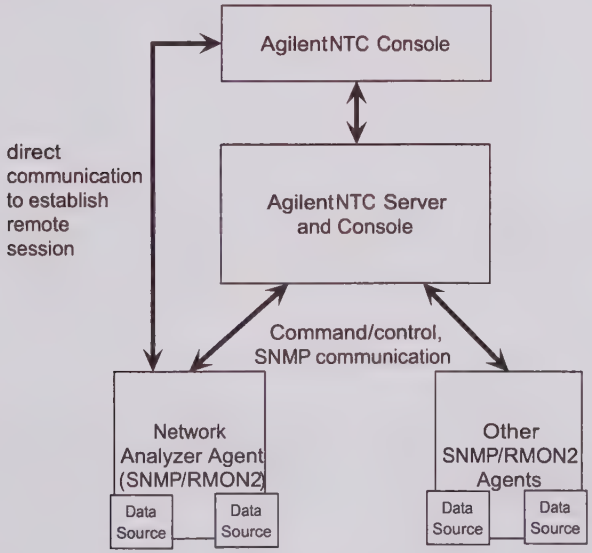
- Access one or more of Agilent's Network Analyzer or Distributed Network Analyzer test products to perform detailed troubleshooting using a remote session window. NTC allows you to quickly access a single test device or centrally access multiple remotely located devices.
- Access and manage an array of other distributed and dispatched network test devices using SNMP. Auto-discover supported SNMP devices.
- Using SNMP, gather MIB-II, RMON, and RMON2 data from a variety of network devices including Network Analyzer and Distributed Network Analyzer products.
- Display historical or real-time SNMP/RMON2 data from multiple data sources in consolidated sliding-time-window data views.
- View specific network events and set up SNMP traps and other actions based on those events.
- Test virtual circuits such as VLANs and WAN PVCs.
- Maintain and access time-relative data from a local database.

The Network Troubleshooting Center supports the entire work flow of network troubleshooting, from time-and-space problem isolation to detailed and localized measurements. NTC provides the test device management and the multi-dimensional view of network data that is so important to today's network administrators and test personnel.

Network Troubleshooting Center Architecture and Components

NTC consists of a number of software components that can be installed on a number of computers and test devices. It is useful to understand NTC's architecture and the components on which it is built to get the most out of this powerful test tool and system.

The following diagram shows a high-level view of NTC's architecture. NTC provides accessibility and control to Agilent Network Analyzer and Distributed Network Analyzer test devices (also known as *agents*) via a remote session window. NTC also allows you to gather MIB-II, RMON, and RMON2 data from Agilent and non-Agilent agents for network troubleshooting.

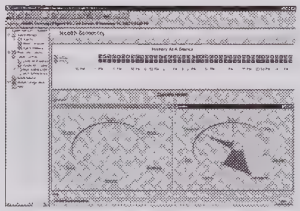


SNMP/RMON2 Data Collection In the SNMP/RMON2 case, SNMP agents gather statistical data from the network under test via their data sources (for example, physical or logical interfaces) and then store that information in a management information base (MIB). The NTC Server then queries these agents to gather network data, which is then displayed in various ways in the NTC Console.

Detailed Network Troubleshooting In the detailed troubleshooting case, the NTC Console provides access (initially via the NTC Server) to Network Analyzer agents outside the SNMP communication path. The user can open a remote session to one of these agents to run detailed Network Analyzer measurements.

The following sections describe each of the components in more detail.

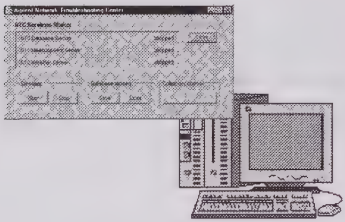
Agilent NTC Console



The Agilent NTC Console is an application used to manage agents (see page 13), to view the results of data collection services run by the server (see below), and to provide access to detailed troubleshooting applications on agents that support them.

The Agilent NTC Console is automatically installed when the NTC Server is installed, but it can also be installed on one or more client computers separate from the server installation.

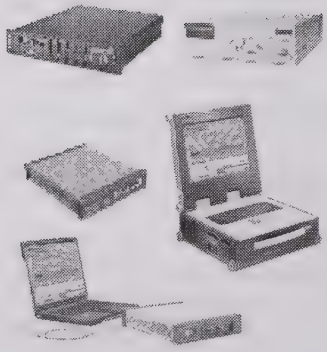
Agilent NTC Server



The Agilent NTC Server is the centralized communication point between NTC Consoles and agents on the network(s) under test. The Server handles detection of threshold violations, events, and agent status, which are stored in the server's data repository and are made available to the Agilent NTC Console. Equally important is the database maintained on the server that holds all collected MIB-II, RMON, and RMON2 data as well as information about agents and their capabilities.

When you purchase NTC, you are allowed to install the NTC Server on one computer, and the Server can collect data from some fixed number of physical interfaces. See chapter 3 for more details on licensing.

Agents



Agents are the devices and/or software processes that NTC accesses, queries, and sometimes controls to gather network metrics, measurement results, and other data. Strictly speaking, agents are not part of NTC, but without agents, NTC would not be able to do its job.

Typically, agents may be widely distributed across a network, and can take many forms. Agents often provide multiple data sources (for example, physical interfaces). The agents supported by NTC are described in the next two sub-sections.

Agilent Network Analyzer Agents

Agilent manufactures a number of test products with which NTC can communicate via SNMP and from which NTC can gather MIB-II, RMON, and RMON2 data. In addition, using NTC, detailed troubleshooting sessions (using the Network Analyzer software) can be run on each of these Agilent agents. Agilent agents include:

- Agilent Distributed Network Analyzer MX
- Agilent Distributed Network Analyzer ME
- Agilent Network Analyzer
- Agilent Distributed Network Analyzer (used with a PC)
- Agilent Network Analyzer Software (installed on a PC)

Refer to the respective Hardware or Software Setup Guides to learn more about each of the above test devices. Also refer to the *Network Analyzer Getting Started Guide* to learn more about the overall Network Analyzer test solution.

Other SNMP Agents

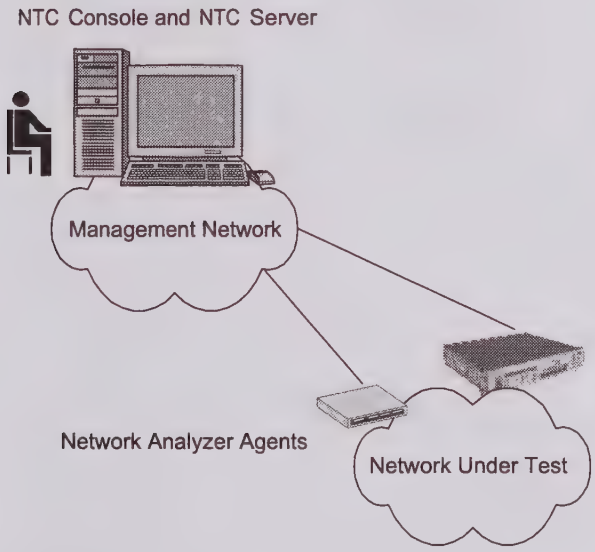
NTC can query a number of other Agilent and non-Agilent devices via SNMP to gather MIB-II, RMON, and RMON2 data. The following list represents those devices that have been tested with NTC, but does not necessarily represent an exhaustive list of the devices from which NTC can collect data.

- Agilent NetMetrix LAN/WAN/ATM Probes
- Cisco Catalyst Switches (1900, 2820, 5000, 5500, 5509, 6500)
- Cisco 7200 Routers
- HP Procurve Switches (224M, 1600M, 4000M, 8000M)
- Network Associates Sniffer Distributed RMON Agents (Frame Relay, FastEthernet)
- HP LaserJet Printers (5M, 8100DN)
- Microsoft SNMP service

Due to variations in third-party implementations of SNMP/RMON2, NTC may not be able to collect data from all devices claiming compliance with SNMP/RMON2 specifications.

Network Troubleshooting Center Deployment

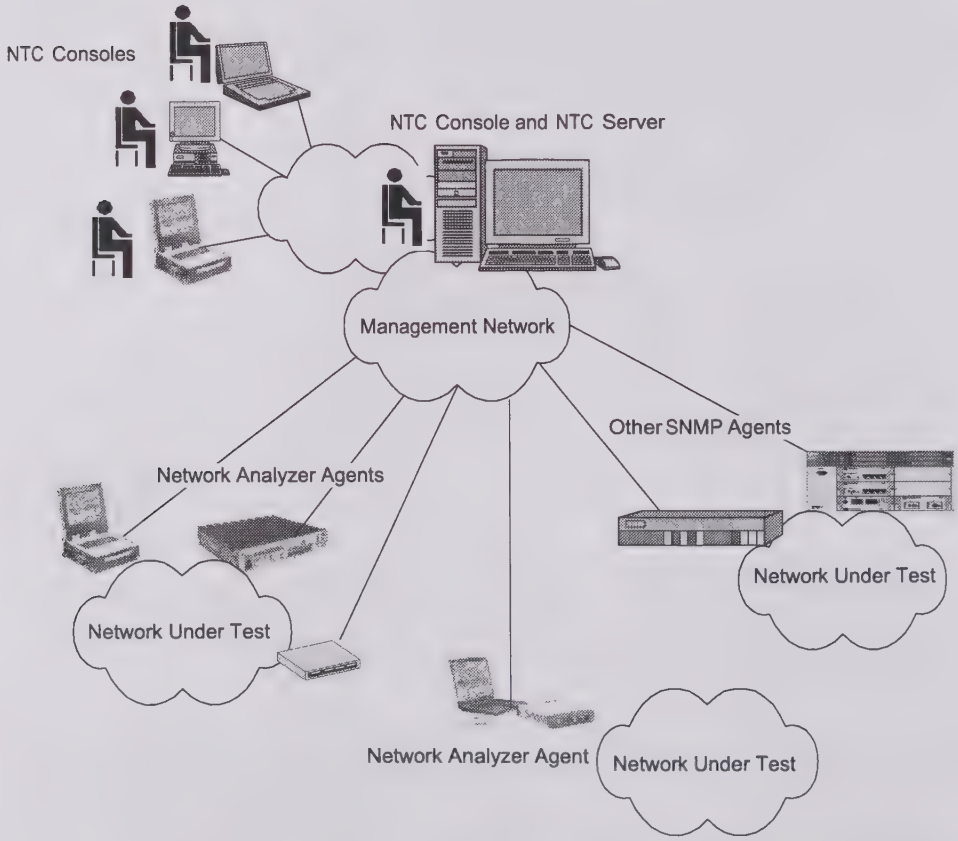
In its simplest deployment, NTC provides direct access to DNA MX and DNA ME test devices as shown below.



In this case, a typical deployment might consist of an NTC Console and Server installation on a single computer and one or more Agilent Network Analyzer and DNA test products deployed locally or remotely to the network under test.

While NTC can be used to gather SNMP/RMON2 data from these Agilent agents, it is usually used to directly access Network Analyzer software on the agents using a remote session window.

For larger enterprise network operators and service provides, a more ambitious deployment is often justified.



As shown, a typical NTC deployment consists of a single NTC Server installation (which includes an NTC console), several optional NTC console installations on computers other than the server host, and a number of Agilent and non-Agilent agents widely dispersed throughout the networks under test.

Note the following about NTC's deployment:

- When multiple NTC Consoles are to access the same NTC Server simultaneously, the Consoles are usually installed at remote locations, allowing test personnel the freedom to monitor and troubleshoot their networks from various places. Each of the Consoles that communicate to the same server displays essentially the same information and provides the access to the same agents, but each can view the available information independently.
- A single NTC Server is licensed for a fixed number of physical interfaces for SNMP/RMON2 data collection. The number of interfaces depends on the product purchased (see chapter 3). The number of agents that can be managed by the NTC Server is not tied directly to the number of interfaces licensed because (1) agents have different numbers of interfaces, and (2) some agent access is not limited by the interface license. Any number of agents can be managed by the NTC software, although simultaneous SNMP data collection will be limited based on the product purchased. See chapter 3 for more information.
- Although often used as an NTC agent (or standalone dispatched test device), the Agilent Network Analyzer can host the NTC Console or the NTC Server or both. Please see chapter 2 for deployment and installation information.

Chapter 2 describes the steps required to deploy NTC as part of Agilent's centralized troubleshooting solution.

Features Overview

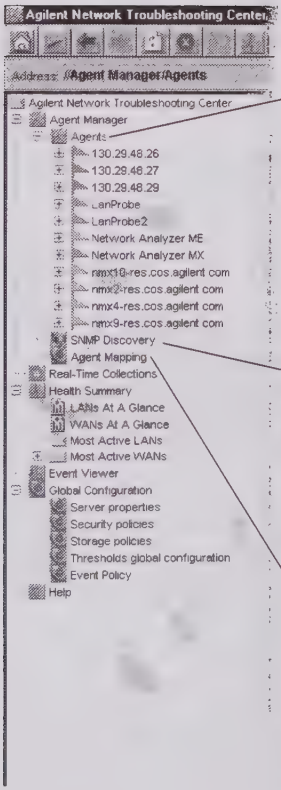
This section provides an overview of the main features of the NTC software:

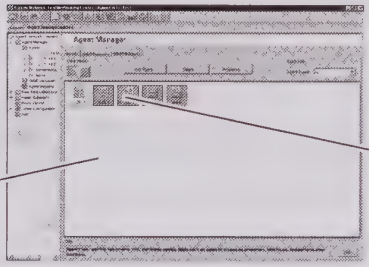
- Agent Management - page 19
- Data Display - page 20
  - MIB-II, RMON, RMON2 Display - page 20
  - Detailed Troubleshooting - page 24
  - Event Viewer - page 25
- Global Configuration - page 26

Refer to the NTC online Help for detailed descriptions of NTC's features and how to use them. Refer to chapter 2 for the steps to deploy the NTC. Refer to chapter 3 for examples of using NTC.

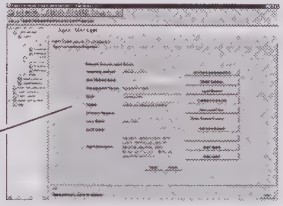
Agent Management

NTC provides robust agent management that includes adding, deleting, and configuring agents. You can also auto-discover agents, access agent interfaces and agent properties, and open remote sessions for detailed troubleshooting (see page 24).]

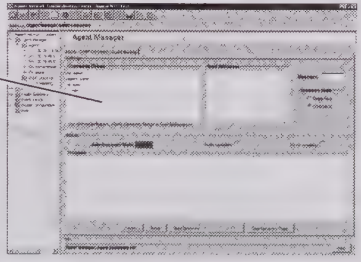




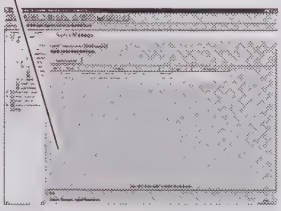
Agents tab - used to add, delete, and manage agents.



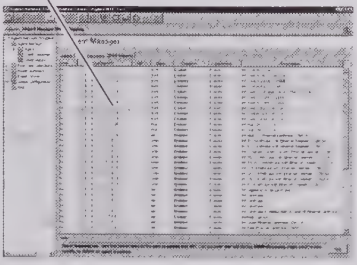
Agent Properties - used to perform most top-level agent management.



SNMP Discovery tab - used to automatically find agents on your network.



Agent Interfaces - used to control data collection and open detailed troubleshooting sessions.



SNMP Mapping tab - used to define agent classes, and discovery/collection policies.

Refer to NTC's online Help for full descriptions of Agent Management capabilities.

Data Display

There are a number of ways network test data is displayed using NTC. NTC provides problem isolation capabilities that lead into detailed and specific network testing on individual devices. In addition, NTC handles the asynchronous traps and events that are very useful for both problem isolation and detailed testing.

The three types of data display NTC provides are:

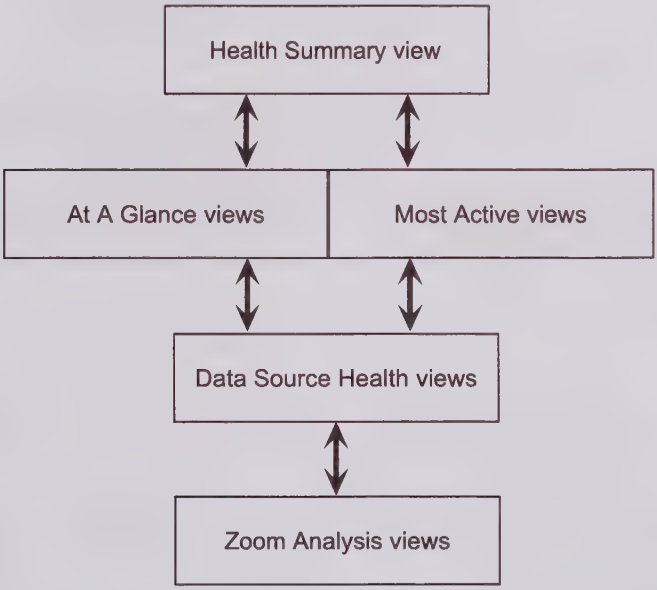
- MIB-II, RMON, and RMON2 data display - see page 20
- Detailed network troubleshooting using a remote session window and agent applications - see page 24
- Event Viewer - see page 25

Overviews of each of these types of data display are provided next. Please refer to the online Help for detailed descriptions of the features and how to use them.

MIB-II/RMON/RMON2 Data Display

The data display views described in this section show MIB-II, RMON, and RMON2 data that is collected from SNMP agents located in the networks under test. These data display views are arranged in a hierarchy that allows you to drill down to more

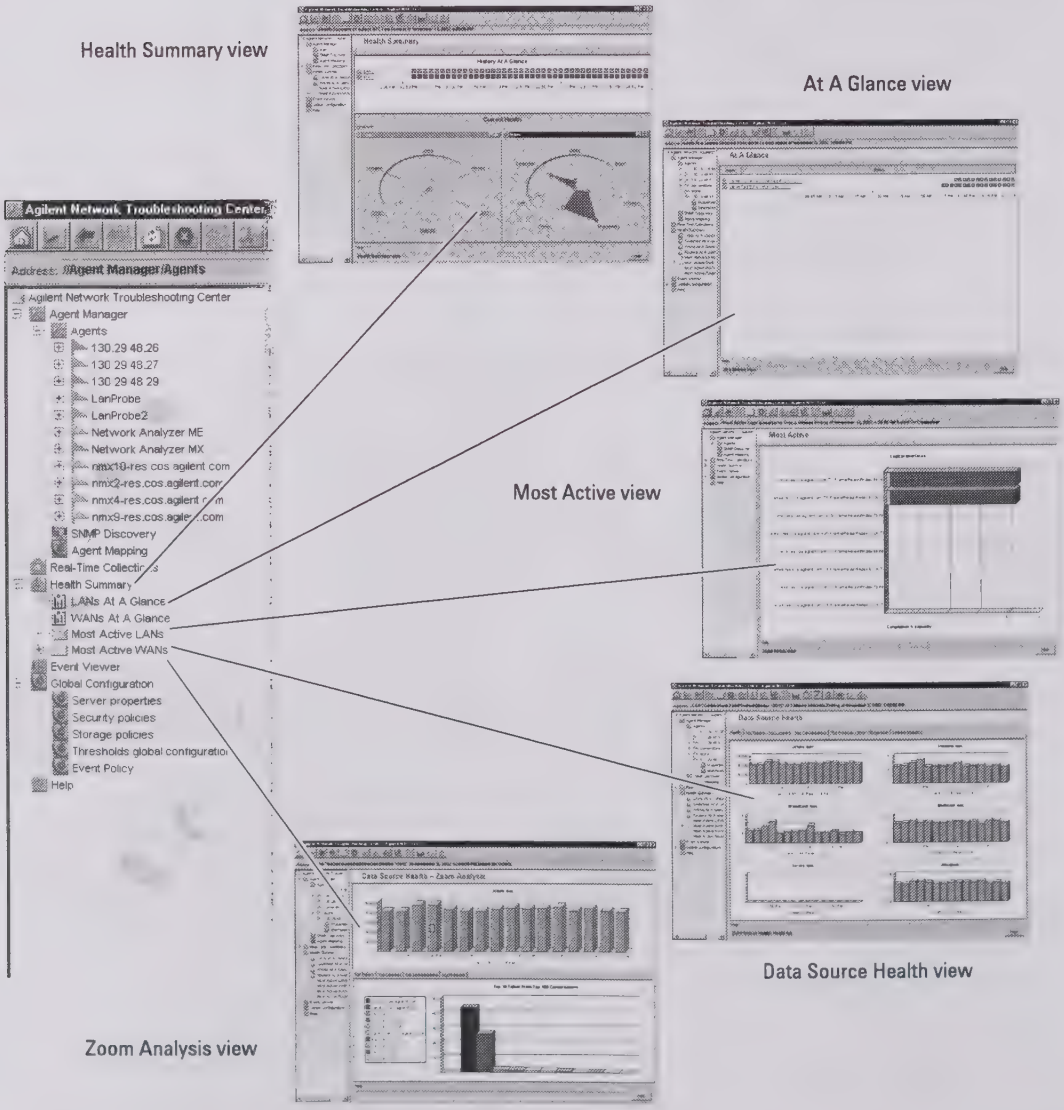
detailed and contextually relevant data. The following diagram demonstrates the basic structure of the views and the order in which you will see them.



The views display collected data in bar graphs, radar graphs, tables, and overview charts. Collected data is presented in context layers that you can navigate to discover the source of network problems.

NTC's MIB-II, RMON, and RMON2 data displays provide a multi-dimensional view into the network by showing data in a sliding time-frame window, sorted according to data sources (or test devices), and with red, yellow, and green indicators to quickly identify and localize trouble. This type of display is well suited to problem isolation.

The following diagram shows the data views provided by NTC. Each view is briefly described on the next page. See the online Help for detailed descriptions and how to use these features.



Health Summary view Shows the overall state of your network with data grouped according to agent type. By clicking hotspots in the view you will see more detailed data either in the At A Glance view or the Most Active view.

At A Glance view Shows the overall state of your network as monitored by a specific class of agents. By clicking labels in this view, you navigate either to another At A Glance view (with more detailed data) or to the Data Source Health view for a specific agent.

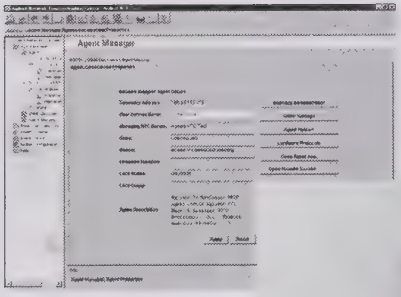
Most Active view Shows the most active data sources (within an agent class) for a given metric. The data sources are sorted from most active to least active. By clicking on a bar in the graph, you navigate to the Data Source Health view for the selected data source.

Data Source Health view Shows a variety of statistics collected from a specific data source. This view has multiple tabs ranging from basic health statistics to very detailed counts of packets, errors, and so on. This view is also used to set up real-time data collections. By clicking on any of the graphs in this view, you navigate to the Zoom Analysis view.

Zoom Analysis view Shows detailed data for the selected metric and the selected time interval, and provides multiple ways to view the same data. The Zoom Analysis view is usually the bottom of the data navigation path for SNMP/RMON2 information.

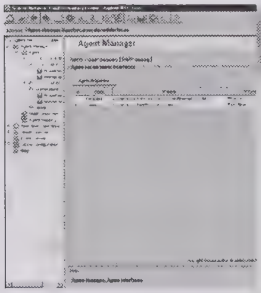
Detailed Troubleshooting with Agent Applications

When using Agilent Network Analyzer agents, you can open a remote session window and run the Network Analyzer software to perform measurements on the agent's interfaces.

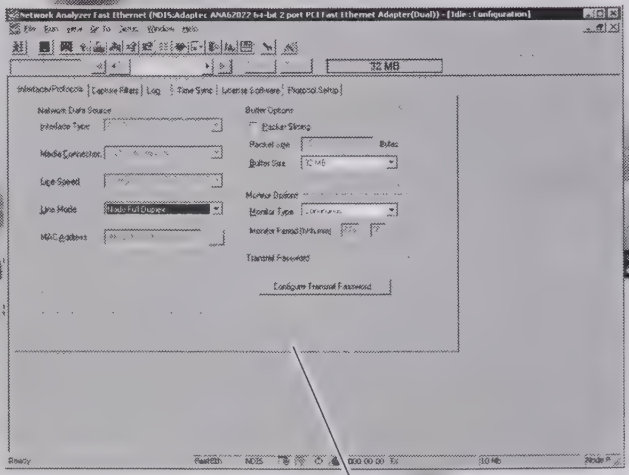


Agent Properties

From the Agent Properties view, Agent Interfaces view, and some data display views, you can start a remote session on the agent and run targeted Network Analyzer measurements.

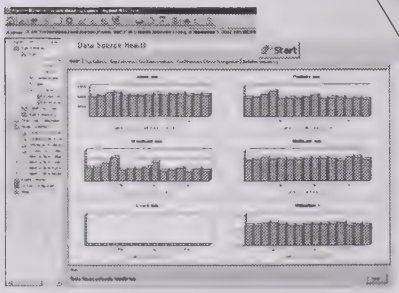


Agent Interfaces



Remote session window

Network Analyzer software

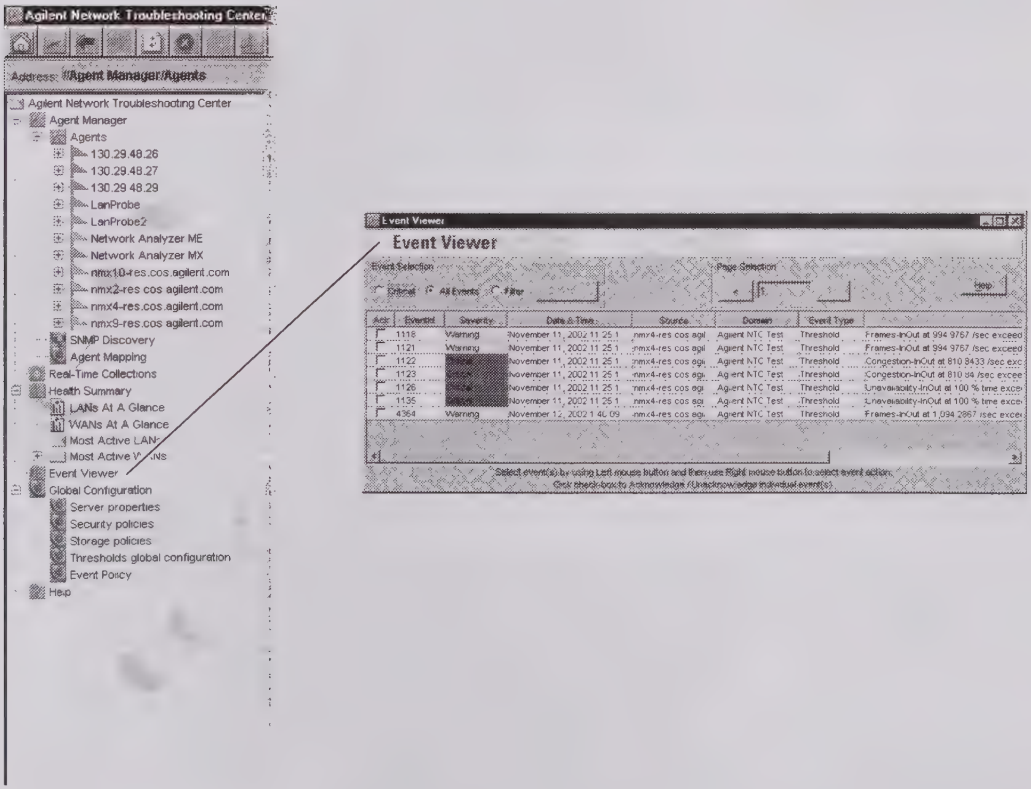


Data Display views

Chapter 2 describes how to start and run targeted network measurements using a remote session window and the Network Analyzer software.

Event Viewer

NTC provides an Event Viewer to monitor warnings, errors, violations, or just changes that have occurred in the NTC Server. Events (and associated information about them) are displayed in a table format and you can sort, filter, and monitor events while viewing other types of data.

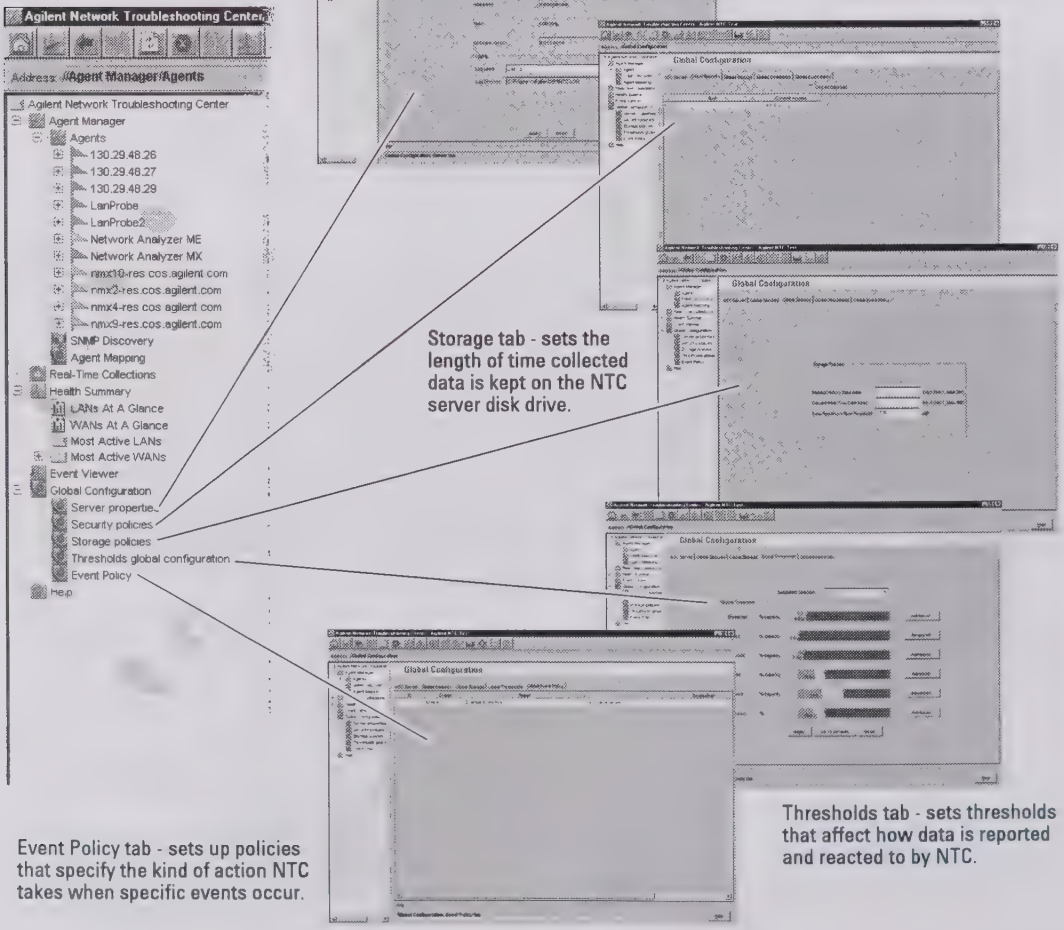

Agilent Network Troubleshooting Center
Address: //Agent Manager/Agents
Agilent Network Troubleshooting Center
Agent Manager
Agents
130.29.48.26
130.29.48.27
130.29.48.29
LanProbe
LanProbe2
Network Analyzer ME
Network Analyzer MX
nmx10-res.cos.agilent.com
nmx2-res.cos.agilent.com
nmx4-res.cos.agilent.com
nmx9-res.cos.agilent.com
SNMP Discovery
Agent Mapping
Real-Time Collections
Health Summary
LANs At A Glance
WANs At A Glance
Most Active LANs
Most Active WANs
Event Viewer
Global Configuration
Server properties
Security policies
Storage policies
Thresholds global configuration
Event Policy
Help
Event Viewer
Event Viewer
Event Selection
Page Selection
Help
Ack
EventId
Severity
Date & Time
Source
Domain
Event Type
1118 Warning November 11, 2002 11:25:1 nmx4-res.cos.agil Agilent NTC Test Threshold Frames-InOut at 994.9757 /sec exceed
1121 Warning November 11, 2002 11:25:1 nmx4-res.cos.agil Agilent NTC Test Threshold Frames-InOut at 994.9757 /sec exceed
1122 November 11, 2002 11:25:1 nmx4-res.cos.agil Agilent NTC Test Threshold Congestion-InOut at 810.8433 /sec exc
1123 November 11, 2002 11:25:1 nmx4-res.cos.agil Agilent NTC Test Threshold Congestion-InOut at 810.84 /sec excee
1126 November 11, 2002 11:25:1 nmx4-res.cos.agil Agilent NTC Test Threshold Unavailability-InOut at 100 % time exce
1135 November 11, 2002 11:25:1 nmx4-res.cos.agil Agilent NTC Test Threshold Unavailability-InOut at 100 % time exce
4364 Warning November 12, 2002 1:40:09 nmx4-res.cos.agil Agilent NTC Test Threshold Frames-InOut at 1,094.2867 /sec exce
Select event(s) by using Left mouse button and then use Right mouse button to select event action.
Click check box to Acknowledge /Unacknowledge individual event(s).

Global Configuration

NTC provides centralized configuration for important data display and server administrative functions.

NTC Server tab - displays and sets important server properties.

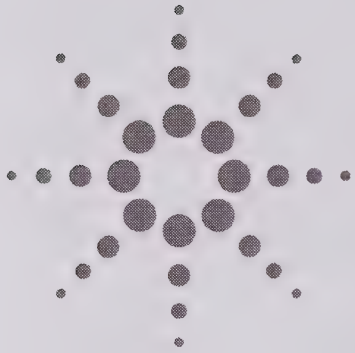
Security tab - restricts access to the server by console IP address or host name.



Storage tab - sets the length of time collected data is kept on the NTC server disk drive.

Event Policy tab - sets up policies that specify the kind of action NTC takes when specific events occur.

Thresholds tab - sets thresholds that affect how data is reported and reacted to by NTC.

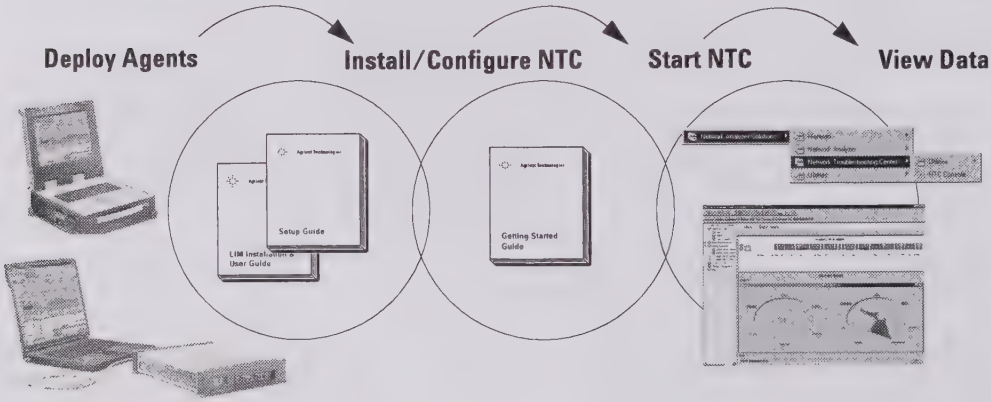


2
Getting Started

Setup Process Overview 28
Deploy Agents 29
Install the Network Troubleshooting Center 34
Start the Network Troubleshooting Center and Begin Testing 37

Setup Process Overview

The following is an overview of NTC's setup process. Each of the main setup steps are covered in more detail in the remaining parts of the chapter in other documentation.



- **Deploy Agents**
  NTC interacts with agents to gather data and allow detailed testing. These hardware and software agents must be deployed and configured to interact with NTC
- **Install and Configure NTC**
  NTC can be installed on a number of computers depending on your test needs.
- **Start NTC**
  You will need to start both the NTC Server and the NTC Console to begin testing.
- **View Data and Start a Remote Troubleshooting Session**
  Once NTC is started, you can add agents, view data and network statistics, and run detailed network troubleshooting applications.

Deploy Agents

Before you can use NTC to monitor and troubleshoot a network, you have to make sure there are supported agents in the network with which NTC can communicate. In some cases, agents might already be deployed and you simply have to add them to NTC (adding agents is discussed on page 42). In other cases, you will have to deploy agents or make sure existing agents are configured to respond to NTC commands.

This section covers the following topics:

- Deploying Agilent Network Analyzer Agents - see page 29
- Deploying Other SNMP MIB-II, RMON, and RMON2 Agents - page 32

This section discusses how to deploy agents and how to make sure existing agents can provide the data necessary to manage and troubleshoot the network under test.

Deploying Agilent Network Analyzer Agents

NTC can communicate with, gather data from, and start detailed remote troubleshooting sessions on a number of Agilent test products. Each of the sub-sections that follow briefly describe how to set up these agents. Refer to the appropriate Hardware Setup Guides for full deployment details.

Distributed Network Analyzer MX and ME

The DNA MX and DNA ME products are intended to be semi-permanently installed in the network to provide SNMP/RMON2 data and detailed Network Analyzer troubleshooting data (via a remote session window).

To deploy a DNA MX or DNA ME:

1 Position the device, install the appropriate Line Interface Module (LIM), connect cables for power, management network, and network under test, and turn the device on.

2 Run the Agent Configuration tool (on another networked PC) to set IP addresses, host names, and a number of other parameters.

The DNA MX and DNA ME immediately start to collect SNMP/RMON2 data that can be made available to NTC. These devices are also immediately able to respond to remote session commands from NTC so you can run the Network Analyzer software on the devices directly.

Network Analyzer and Network Analyzer Software

Both the Network Analyzer tester and the Network Analyzer Software are intended to be used primarily as dispatched test tools but can easily perform as agents in the NTC environment.

To deploy a Network Analyzer dispatched tester as an NTC agent:

1 Position the tester, make sure the appropriate LIMs are installed, connect cables for power, management network, and network under test, and turn the tester on.

2 For an existing Network Analyzer, make sure it has the appropriate software version and operating system to work with NTC.

3 If necessary, use the features of the Windows operating system on the tester to set IP addresses, the host name, and other networking parameters.

4 Use the NTC Agent Services utility to start the services necessary to make the Network Analyzer respond to SNMP queries from NTC.

To deploy the Network Analyzer Software (installed on a non-Agilent PC) as an NTC agent:

1 Identify the PC (that has an appropriate NDIS network interface card) on which the Network Analyzer Software is to be installed. **Note:** Check the PC's operating system and performance requirements.

2 Install the NTC software.

3 If necessary, use the features of the Windows operating system on the PC to set IP addresses, the host name, and other networking parameters.

4 Using the Windows operating system:
a) Create or verify an appropriate user account and password if necessary.
b) Enable the Windows Remote Desktop and make sure the target user is authorized to use the Remote Desktop.
c) Disable "Fast User Switching".

5 Use the NTC Agent Services utility to start the services necessary to make the PC (with the Network Analyzer Software installed) respond to queries from NTC.

Distributed Network Analyzer

Among other things, the Distributed Network Analyzer (DNA) is designed to provide an additional Line Interface Module (LIM) to DNA MX, DNA ME, Network Analyzer, and PC-based Network Analyzer products.

To deploy a Distributed Network Analyzer:

1 Set up the PC, DNA MX/ME, or Network Analyzer to which the DNA will be connected (see above steps). Connect the DNA to the controlling device.

2 Use the Agent Configuration tool to set DNA IP addresses and/or to associate the DNA with the controlling device (that is, set its "owner").

Importance of Setting Time Zones on Agents

The operating system time zone for the Network Analyzer dispatched tester and Distributed Network Analyzer MX and ME testers is set to Greenwich Mean Time (GMT) at the factory. Using the GMT time zone setting is particularly important in centralized network troubleshooting cases where you are capturing data from geographically dispersed networks and network test equipment. In those cases, setting the time zone to GMT for each of the data collection devices allows you to correctly and easily analyze the correlated data.

It is recommended that you also set the operating system time zones on the NTC Console and NTC Server computers to GMT as well. This will ensure that all components of the test system use the same time stamps.

DHCP versus Static IP Address Configuration

The DNA MX and the DNA ME may be configured to use DHCP to acquire their IP addresses, or may be configured with static IP addresses. The Network Troubleshooting Center may also be run on hosts using either DHCP or static IP addresses.

Although DHCP is supported by these systems, for the most reliable system performance it is recommended that static IP addresses be used for all NTC agents, as well as for the NTC Server. Hosts running NTC Consoles can use either IP address configuration mechanism equally well.

Deploying Other SNMP MIB2, RMON, and RMON2 Agents

It is beyond the scope of this *Getting Started Guide* to describe in detail how to deploy, or verify the deployment of, the large number of SNMP MIB-II, RMON, and RMON2 agents from which NTC can gather data. Below, however, is a list of known supported agents and some tips on how to make sure they provide the best information for NTC.

Supported Agents

The following agent types have been tested with NTC:

- Agilent NetMetrix LAN/WAN/ATM Probes
- Cisco Catalyst Switches (1900, 2820, 5000, 5500, 5509, 6500)
- Cisco 7200 Routers
- HP Procurve Switches (224M, 1600M, 4000M, 8000M)
- Network Associates Sniffer Distributed RMON Agents (Frame Relay, FastEthernet)
- HP LaserJet Printers (5M, 8100DN)
- Microsoft SNMP service

This is not an exhaustive list of agents that NTC might be able to gather data from. Generally, any device that implements standard SNMP MIB-II, RMON, and RMON2 can be queried by NTC. However, due to the variations in the way vendors implement SNMP/RMON2, NTC may not be able to collect data from all devices claiming compliance with the specifications. You can add or discover other agent types but Agilent does not guarantee their effectiveness as data collection devices when used with NTC.

NOTE

For devices not accounted for in NTC's SNMP Mapping tab, you might need to add a mapping policy for these devices to be discovered.

Install the Network Troubleshooting Center

This section provides a brief overview of NTC's installation process. Full installation instructions appropriate for specific hardware can be found in the Network Analyzer Hardware Setup Guides and the *Network Troubleshooting Center / Network Analyzer Software Setup Guide*.

As you prepare to install NTC (and during the installation), keep the following items in mind:

- **Installing the NTC Console vs. Server and Interface Licensing**
  Remember that you can install the NTC Console and Server on a single computer and you can install the NTC Console (without the Server) on several computers. Also, the NTC product you purchased is licensed for data collection on a fixed number of physical interfaces. This licensing limit affects how many agents from which you can simultaneously collect data. See chapter 3 for more details.
- **Before you install NTC**
  Some logistical items to consider prior to installation:
  - For performance reasons, you should not install the NTC Server on a computer that is heavily used for another purpose, such as a Web server, a file server, or a domain name server.
  - It is recommended that you install Agilent NTC on NTFS for better security, system failure recovery, and performance. You can install Agilent NTC on FAT or FAT32 as well. (NTFS, FAT, and FAT32 are operating system file formats. See your Windows documentation for more information.)

- If you have been using a previous version of NTC, you may want to keep the data (that is, the database) you have collected before installing the new version. If the new version of NTC is installed in a different location than the previous version, the previous database will not be overwritten or altered in any way. However, if the new version is installed over the old version, note the following:
  (1) If the old database and the new database are compatible, NTC will use the previous version, preserving saved data and appending new data into the database.
  (2) If, however, the databases are incompatible, the old database will be overwritten and all previous data will be destroyed. In this case, you might want to back up your previous database before installing NTC. See the online Help for more information.
  Saved versions of older databases may not work with the newer version of NTC.
- Check the installation requirements of the computer on which NTC is to be installed. Also, note that there are higher performance requirements for increased numbers of data collections. Please see chapter 3 for more information.
- As is true of most installations, be sure to stop all processes and exit all programs prior to installing NTC. This includes anti-virus software.
- Note the IP address and/or the host name of the computer on which you will install the NTC Server. You will use this IP address (or host name) when you log in to NTC to begin monitoring and troubleshooting. If you intend to install NTC on a "multi-homed host" (that is, a computer with multiple network interface cards and, therefore, multiple IP addresses), be aware that the NTC Server will be associated with only one of these IP addresses. You can control which IP address with which the Server will be associated. See NTC's online Help for NTC Server Manager for more information.

- **Installation Process**
  NTC is installed from a single CD that includes Network Analyzer software and other utilities. Please refer to the *Network Analyzer / Network Troubleshooting Center Software Setup Guide* to make decisions about what to install and on which devices to install it.
- **Integrating with Network Management Stations**
  NTC can interact with third-party NMSs such as HP OpenView. There are separate installation procedures to address this need. Please see chapter 3 for more information.
- **Starting the Server after the installation**
  After the NTC Server installation, you are asked if you want to start the NTC Server automatically. It is usually a good idea to do this, but if you do not intend to immediately add agents, start data collection, or start a remote session, you can start the Server later using the Manage NTC Server option in the Windows start menu.
- **Uninstalling NTC and Saving the NTC Database**
  If you want to uninstall the NTC Server, you might want to back up the database. Use the Manage NTC Server option in the Windows Start menu. In addition, you should run the Pre-Uninstall utility in the Start menu.

Start the Network Troubleshooting Center and Begin Testing

This section shows you how to start and run NTC once it is installed. Generally, the start-up process involves the following steps:

- Start the NTC Server (if necessary) - see page 37
- Start the NTC Console - see page 39
- Add or discover agents - see page 42
- Gather and view SNMP/RMON2 data from the agents - see page 54
- Start detailed remote troubleshooting sessions on agents that support them - page 57

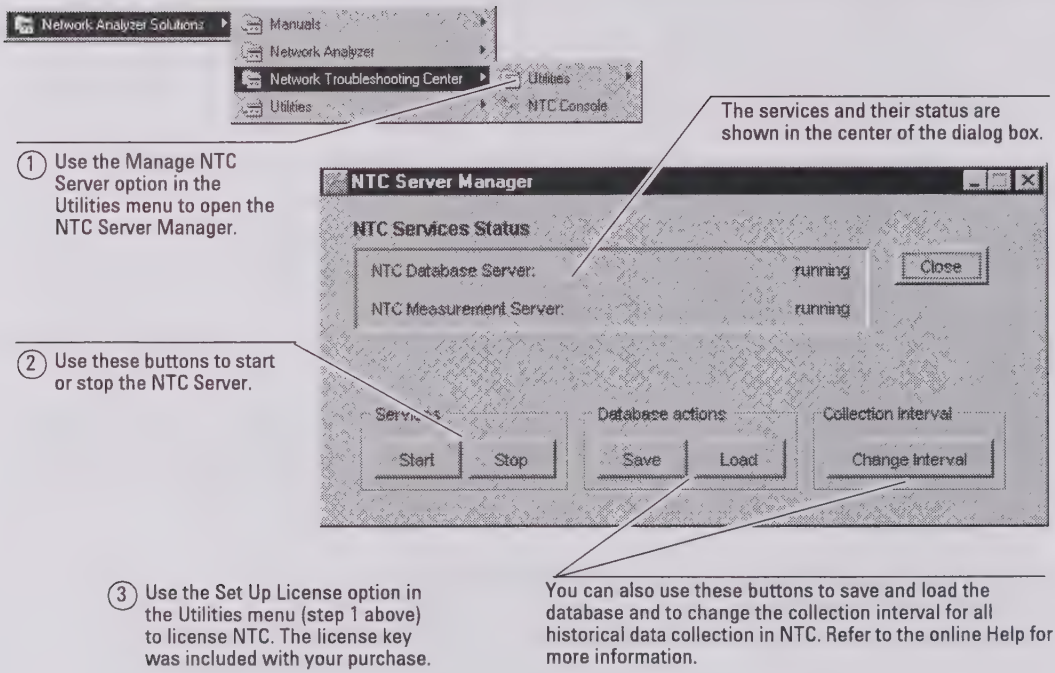
Not all of the above steps (which are covered in more detail in the following pages) are required every time you run NTC. Some steps can be skipped as you become more familiar with NTC's operation.

Starting and Stopping the NTC Server

When installing the NTC Server, you can choose to start the Server immediately and you can configure it to start automatically every time the Server computer is turned on or rebooted. However, there are situations in which you will have to start (or stop) the NTC Server outside of the installation process or verify that it is running before starting the NTC Console. In addition, the NTC Server provides database maintenance capabilities and allows you to change data collection intervals.

NOTE

It is recommended that you close the NTC Console before stopping the services because an error will display when the services are stopped.


Network Analyzer Solutions
Manuals
Network Analyzer
Network Troubleshooting Center
Utilities
Utilities
NTC Console
1 Use the Manage NTC Server option in the Utilities menu to open the NTC Server Manager.
The services and their status are shown in the center of the dialog box.
NTC Server Manager
NTC Services Status
NTC Database Server:
running
NTC Measurement Server:
running
Close
2 Use these buttons to start or stop the NTC Server.
Start
Stop
Database actions
Save
Load
Collection Interval
Change Interval
3 Use the Set Up License option in the Utilities menu (step 1 above) to license NTC. The license key was included with your purchase.
You can also use these buttons to save and load the database and to change the collection interval for all historical data collection in NTC. Refer to the online Help for more information.

Note the following about starting and stopping the NTC Server:

- The NTC Server runs in the background on the Server computer. To use the NTC Server window (shown above), you will have to open it using the Start menu in the Server computer's Windows desktop. You cannot open the NTC Server window remotely.
- If the NTC Server is not running when you attempt to start the NTC Console, you will see an error message.
- Reasons to stop the NTC Server include needing to back up the database, changing the collection interval, performing an NTC Server upgrade, and so on.
- Closing the NTC Server window (using the Close button) does not stop the Server.

Starting the NTC Console

The NTC Console is used to access the NTC Server and agents for most data display and troubleshooting tasks. Remember the following items when you start the Console:

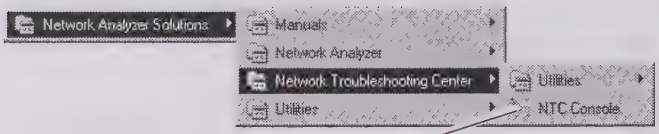
- Multiple Consoles can access the same NTC Server simultaneously. Therefore, the same Server configurations and data collection conditions are viewed by all of the connected Consoles. This includes agents that have been added, collection intervals, and collected data. Each Console can view data and configurations independently, but each will display the same information when viewing the same display or configuration views.
- Unless limited by the Security tab in Global Configuration, all Consoles have the same control over the Server. Thus, one Console can over-write configurations set by another Console.
- Essentially, there is no difference between accessing the Server with the Console running on the same computer or with one running on a remotely located computer, except performance considerations on the network between the Console and Server.

Use the procedure on the following pages to start an NTC Console.

NOTE

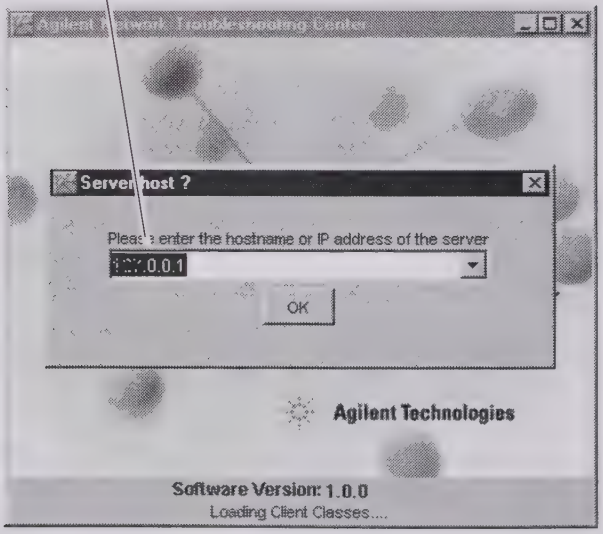
Prior to starting the NTC Console, you might need to license NTC. You do this at the NTC Server computer using the Set Up License option in the Network Troubleshooting Center | Utilities menu. If you do not license NTC, you will get an error message when you attempt to start the Console.

When starting the NTC Console, you have to specify the NTC Server to which the Console will connect.



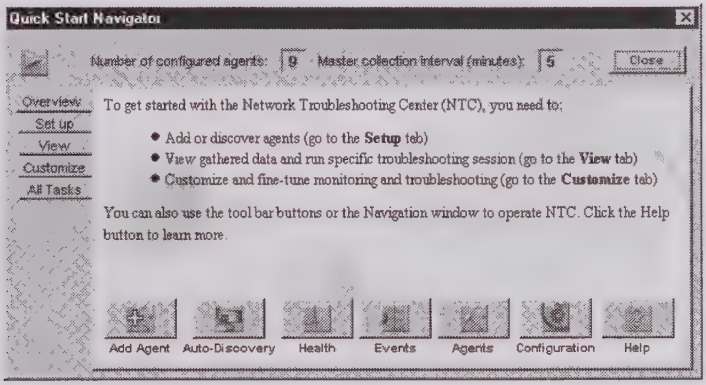
(1) Use the NTC Console option in the Start menu.

(2) Type in the IP address or host name of the NTC Server to which the Console will be connected. If you are starting the Console on the same computer on which the Server is installed, and intend to connect to that Server, you can use the well-known "localhost" IP address 127.0.0.1.



If the NTC Server that you want to connect to is installed on a "multi-homed host" (that is, a computer with multiple network interface cards and, therefore, multiple IP addresses), the IP address you type in is determined by the operating system of the host computer. To learn how to change the IP address with which the Server is associated, see NTC's online Help for NTC Server Manager.

After you have specified the NTC Server, the Console window opens with the Quick Start Navigator on top.


Quick Start Navigator
Number of configured agents: 9
Master collection interval (minutes): 5
Close
Overview
Set up
View
Customize
All Tasks
To get started with the Network Troubleshooting Center (NTC), you need to:
Add or discover agents (go to the Setup tab)
View gathered data and run specific troubleshooting session (go to the View tab)
Customize and fine-tune monitoring and troubleshooting (go to the Customize tab)
You can also use the tool bar buttons or the Navigation window to operate NTC. Click the Help button to learn more.
Add Agent
Auto-Discovery
Health
Events
Agents
Configuration
Help

The Quick Start Navigator serves two purposes:

- It provides an overview of how to use NTC.
- It provides quick access to NTC's main functions.

You can access the Quick Start Navigator any time you need to by using the toolbar button in the upper left corner of the NTC Console window.

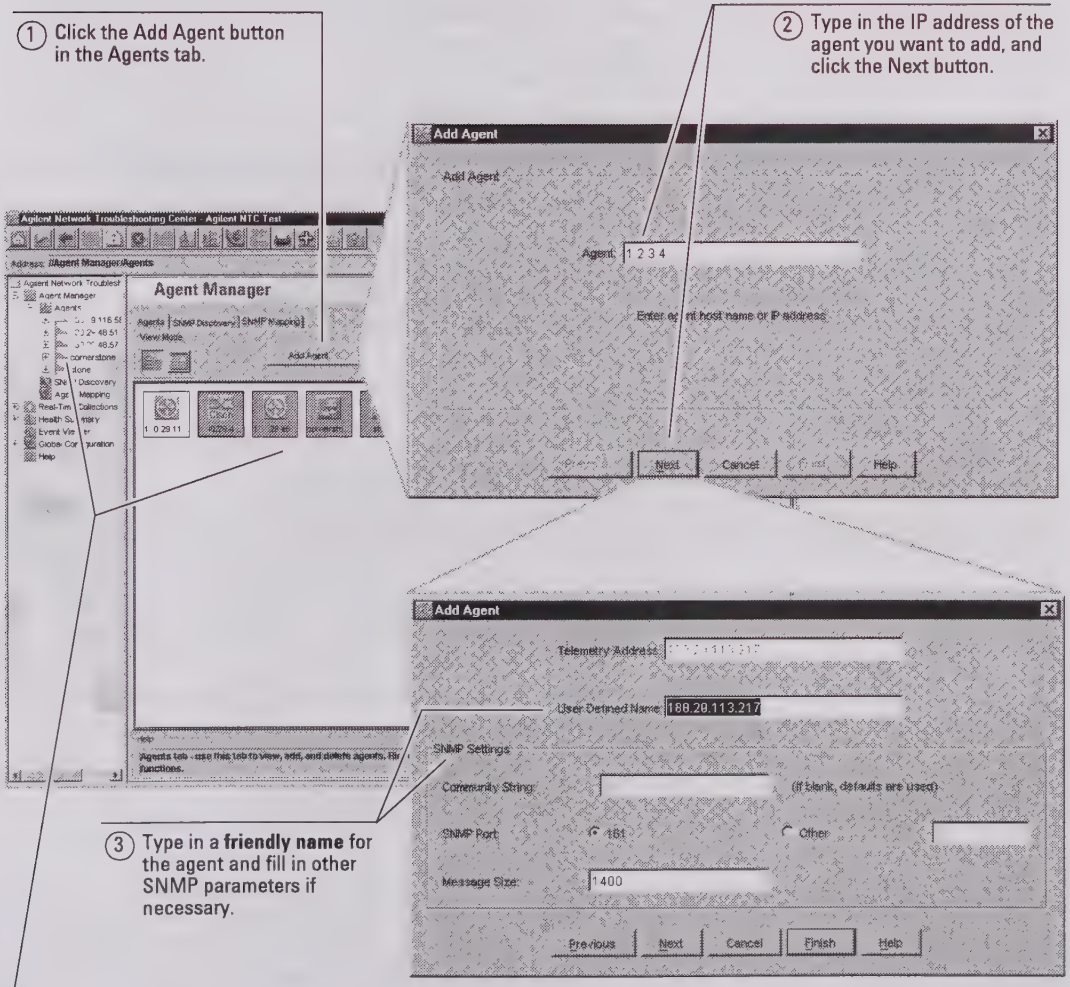
Adding, Discovering, and Managing Agents

NTC must interact with agents to gather and display data and to provide access to detailed network troubleshooting applications. Therefore, often the first thing you do once you have started the NTC Console is to add, discover, or manage agents. This section describes how to:

- **Manually Add Agents**
  You manually add agents if you have a relatively small number of them to add. This is the method often used when you are using NTC to access a small number of Agilent's Distributed Network Analyzer MX and Distributed Network Analyzer ME test devices. See page 43 to learn more.
- **Discover Agents**
  You discover agents when you have a large number of them to add or are relatively unfamiliar with agents deployed across the network under test. See page 45 to learn more.
- **Manage Agents**
  Once you have added and/or discovered agents, you will need to manage them and access specific troubleshooting capabilities on them, including running remote troubleshooting sessions (see page 57) on Network Analyzer test equipment such as the DNA MX, DNA ME, and others. See page 47 to learn more.

Manually Adding an Agent

Use the following procedure to manually add an agent.



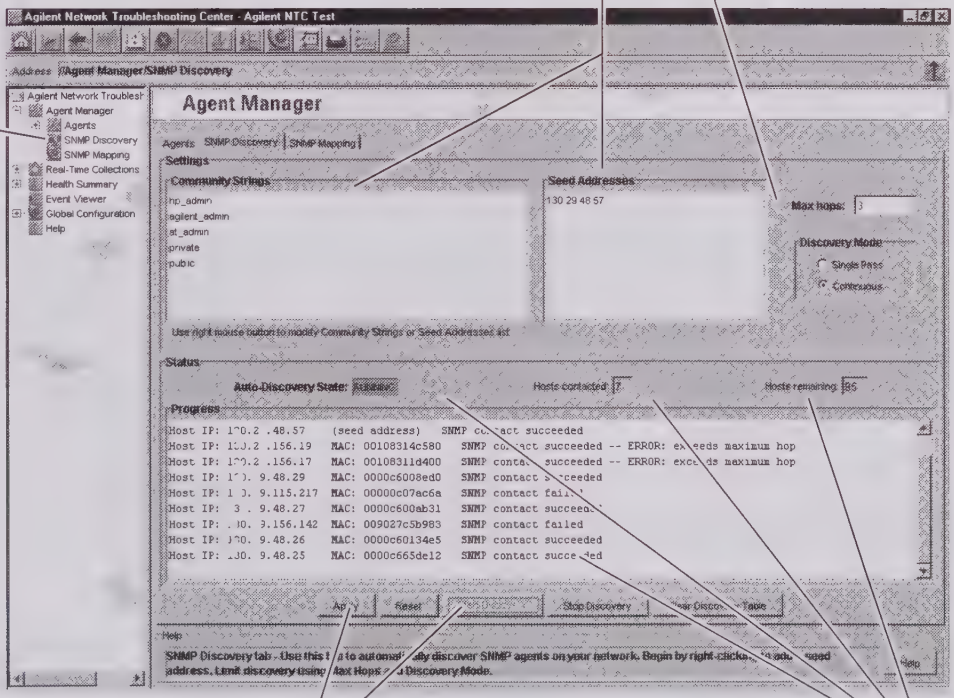
Once NTC finds and successfully adds the agent, an agent icon is displayed in the Agents tab and an entry is placed into the Navigation tree. You can monitor the status of added agents using the icon colors and you can select which subset of agents to view using the Agent Filter list box in the Agents tab.

Note the following items concerning manually adding agents:

- To manually add an agent, you must know the agent's IP address. In addition, you must know the agent's SNMP community string, SNMP port number, and SNMP message size if the agent uses non-standard values. Usually NTC's defaults are adequate.
- After the agent is added, you can monitor its state by looking at the agent icon colors or using the State column in the tabular view. You can also filter which agents you want visible using the Agent Filter list box. Refer to the online Help for more details.
- After an agent is added, and if NTC is configured to start collection on that agent automatically (see SNMP Mapping on page 53) at least two collection intervals will pass before SNMP/RMON2 data begins to appear in the data display views. Note that for the basic NTC license that allows data collection on 4 physical interfaces, auto-collection is disabled. This means that once you add agents, you will have to manually start collections either in the Agent Properties view or the Agent Interfaces view.
- After the agent is added, you can access Agent Properties to perform multiple functions including starting a remote troubleshooting session (see page 57), and you can access Agent Interfaces to start or stop data collection and add other interfaces. Go to "Managing Agents and Accessing Agent-based Functionality" on page 47 for more information.
- Remember that when agents are added, they are added to the NTC Server database. Therefore, unless they are explicitly deleted, you can close and reopen the Console and the agents will still be available to you.

Discovering Agents

Use the following procedure to discover agents:


Agilent Network Troubleshooting Center - Agilent NTC Test
Agent Manager
Agents
SNMP Discovery
SNMP Mapping
Settings
Community Strings
hp_admin
agilent_admin
at_admin
private
public
Seed Addresses
130 29 48 57
Max Hops:
Discovery Mode
Single Pass
Continuous
Use right mouse button to modify Community Strings or Seed Addresses list
Status
Auto-Discovery State:
Hosts contacted:
Hosts remaining:
Progress
Host IP: 130.2 .48.57 (seed address) SNMP contact succeeded
Host IP: 130.2 .156.19 MAC: 00108314c580 SNMP contact succeeded -- ERROR: exceeds maximum hop
Host IP: 130.2 .156.17 MAC: 00108311d400 SNMP contact succeeded -- ERROR: exceeds maximum hop
Host IP: 130. 9.48.29 MAC: 0000c6008ed0 SNMP contact succeeded
Host IP: 130. 9.115.217 MAC: 00000c07ac6a SNMP contact failed
Host IP: 130. 9.48.27 MAC: 0000c600ab31 SNMP contact succeeded
Host IP: 130. 9.156.142 MAC: 009027c5b983 SNMP contact failed
Host IP: 130. 9.48.26 MAC: 0000c60134e5 SNMP contact succeeded
Host IP: 130. 9.48.25 MAC: 0000c665de12 SNMP contact succeeded
Apply
Reset
Stop Discovery
Help
SNMP Discovery tab - Use this tab to automatically discover SNMP agents on your network. Begin by right-clicking to add seed address. Limit discovery using Max Hops and Discovery Mode.
Stop

1. Use the Navigation tree to go to the SNMP Discovery tab.
2. Add a seed address by right-clicking in this area and using the dialog box that is displayed. A router IP address is usually a good choice. You can add new community strings as well.
3. Set the Max Hops and Discovery Mode parameters.
4. Click the Apply button and then click the Start Discovery button once you have the configuration parameters set.

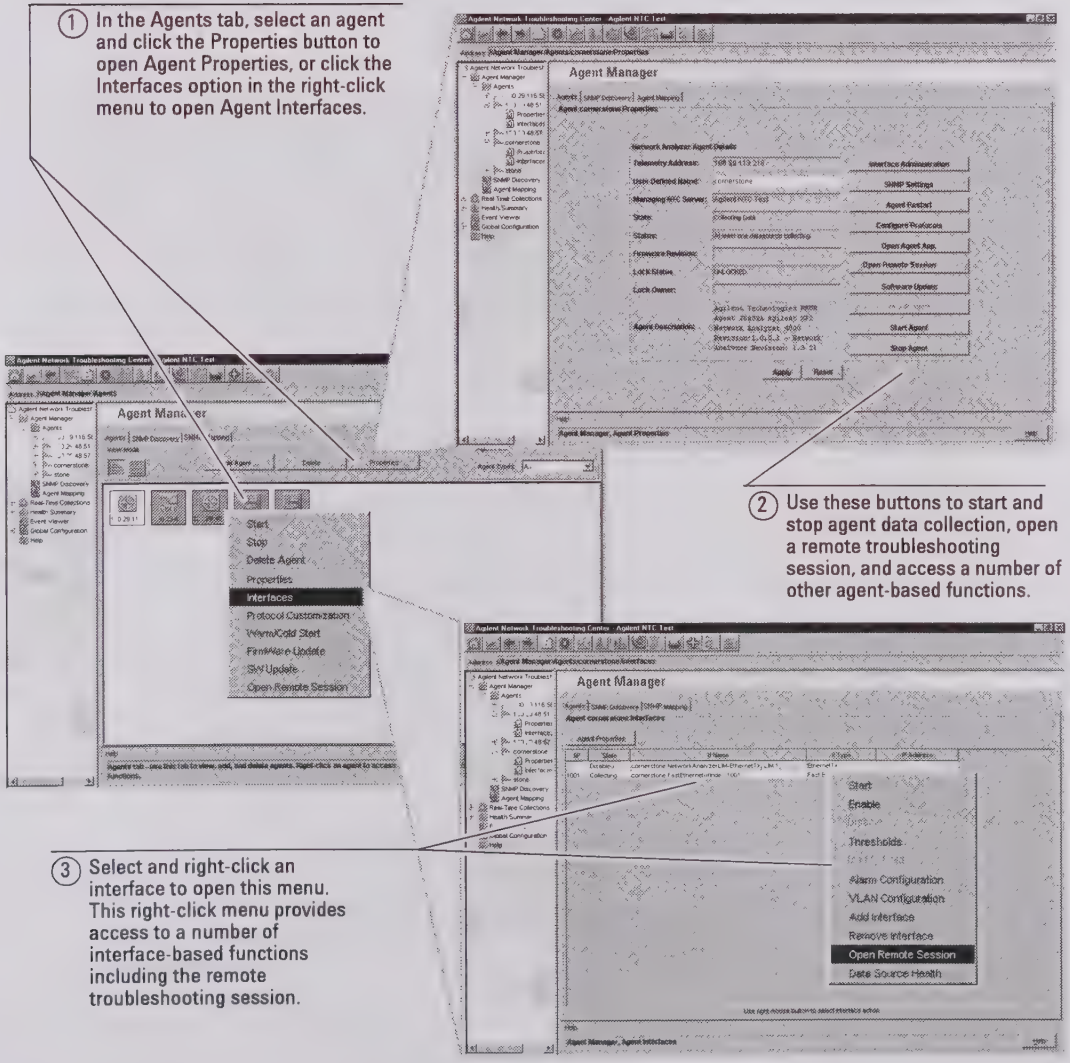
The Status and Progress areas of the SNMP Discovery tab update as agents are contacted. Agents that meet the criteria set in the SNMP Mapping tab (see page 47) are added to the Agents tab. There you can monitor the agent's status using icon color, and you can use the Agent Filter option to make agents only of a certain type visible in the tab.

Note the following items concerning discovering agents:

- Whether an agent is actually added once discovered, or whether the agent will automatically start collecting data depends on the configuration in the SNMP Mapping tab and the license being used. See page 53 for more information.
- Similar to the manual add process, once an agent is discovered and added:
  - You can monitor the agent's state by looking at the agent icon colors or using the State column in the tabular view. You can also filter which agents you want visible using the Agent Filter list box.
  - Two collection intervals will pass before SNMP/RMON2 data begins to appear in the data display views for the newly discovered agent.
  - You can access Agent Properties to perform multiple functions including starting a remote troubleshooting session (see page 57), and you can access Agent Interfaces to start or stop data collection and add other interfaces. Go to "Managing Agents and Accessing Agent-based Functionality" on page 47 for more information.
  - Agents are added to the NTC Server. Therefore, unless they are explicitly deleted, they will be available to the Console on subsequent uses, and to all other Consoles accessing the Server.
- Discovering agents can be a time consuming process. Be aware that the Max Hops and Discovery Mode parameters can affect the discovery time. See the online Help for more details.
- You can limit the discovery process to specific sub-nets to target your search and to limit search time. See the online Help for more details.

Managing Agents and Accessing Agent-based Functionality

This section shows how to access NTC's most important agent-based functions. See the online Help for more details.

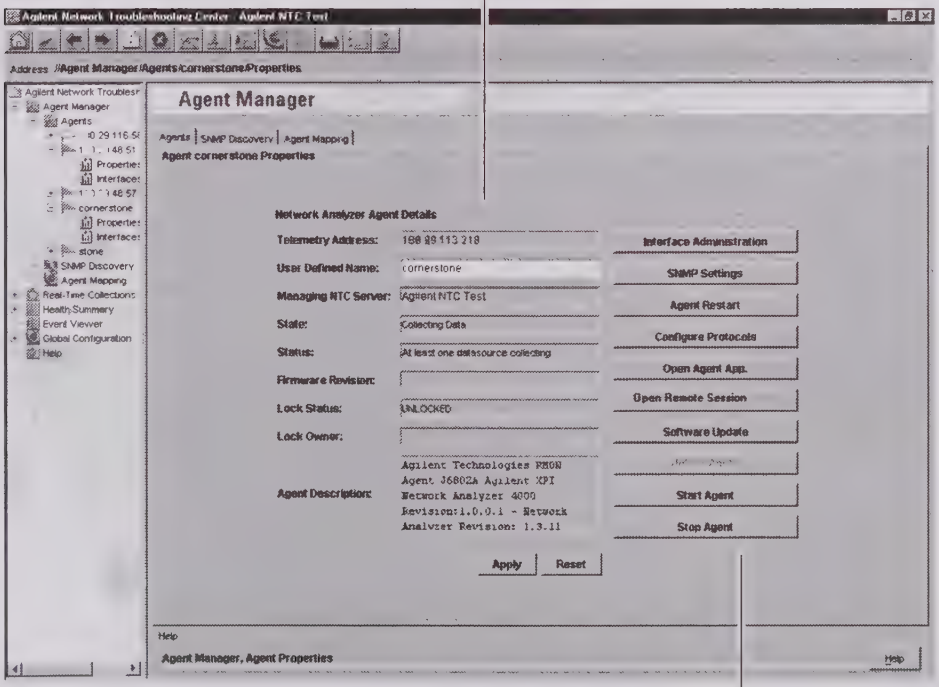

1 In the Agents tab, select an agent and click the Properties button to open Agent Properties, or click the Interfaces option in the right-click menu to open Agent Interfaces.
Agent Manager
2 Use these buttons to start and stop agent data collection, open a remote troubleshooting session, and access a number of other agent-based functions.
Start
Stop
Delete Agent
Properties
Interfaces
Protocol Customization
Warm/Cold Start
Firmware Update
Snif Update
Open Remote Session
Agent Manager
Start
Enable
Thresholds
Alarm Configuration
VLAN Configuration
Add Interface
Remove Interface
Open Remote Session
Data Source Health
3 Select and right-click an interface to open this menu. This right-click menu provides access to a number of interface-based functions including the remote troubleshooting session.

Note the following:

- Every agent that is added or successfully discovered has its own Agent Properties view and Agent Interfaces view.
- Agent Properties and Agent Interfaces are the main starting points for most agent-based functions and capabilities in NTC. Each of these views is covered in more detail in the pages that follow.
- You can easily navigate back to top level of the Agents tab by using the Back button in the toolbar or by using the Navigation tree on the left side of the Console.
- Remember that the right-click menu provides a shortcut to many of the functions that are otherwise accessed from either Agent Properties or Agent Interfaces.

Agent Properties is used to access agent-based monitor and test functions and view agent descriptions and other characteristics.

The center section of the Agent Properties view provides information about the agent and its status.



These buttons are used to open the Agent Interfaces view, open a remote troubleshooting session, and start/stop data collection on all of the interfaces associated with this agent. Refer to the online Help for detailed descriptions of these and other features.

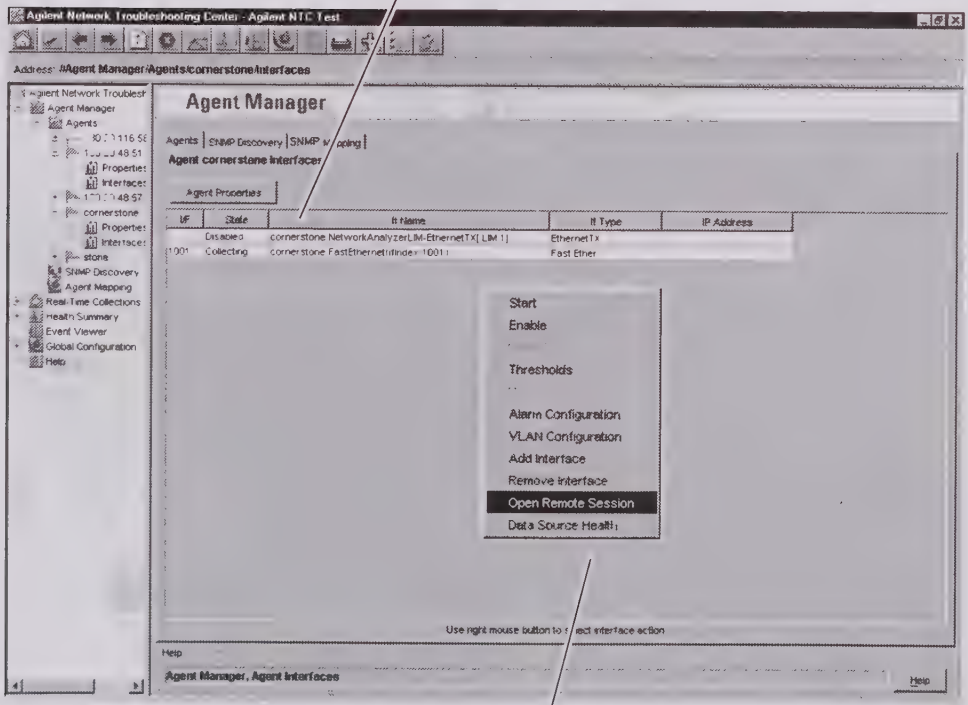
You can do the following from the Agent Properties view:

- To navigate to the Agent Interfaces view, click the Interface Administration button.
- To start and stop data collections on all enabled agent interfaces, click the Start Agent Collection or Stop Agent Collection buttons.
- To open a remote session to run a detailed troubleshooting application, click the Open Remote Session button. To set a user name and password to allow remote access to the agent, click the Remote Session Configuration button.
- To update agent software or firmware, click the appropriate buttons.
- To set SNMP parameters, customize agent protocols, unlock the agent, do a warm/cold start, or perform other functions, click the appropriate buttons.

The fields and buttons in this view depend on the agent type and whether it supports certain functions.

Agent Interfaces is used to view all agent interfaces and to access interface-based monitor and test functions.

Each row in the Agent Interfaces view shows the type of interface, its state (collecting or not), and other important information. In some cases, you can alter information in an interface row to enable other types of data collection.



By selecting and right-clicking an interface, you open the right-click menu from which a variety of interface-based functions can be selected. The menu options depend on the type of interface.

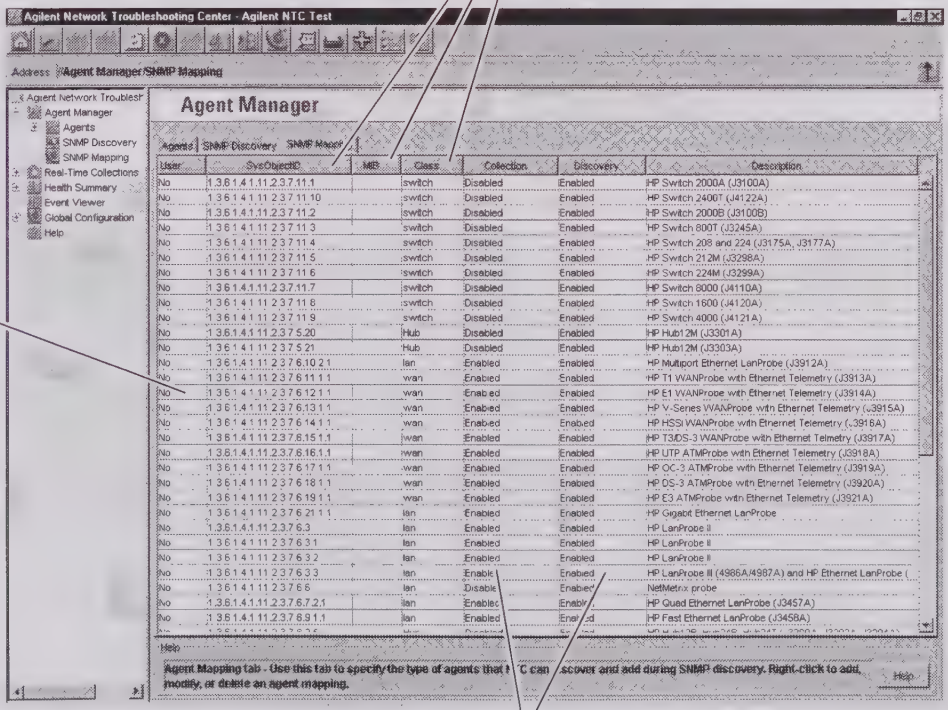
From the Agent Interfaces view you can:

- View the number, type, and status of all interfaces associated with an agent.
- Enable or disable the interface, and start or stop collections using the right-click menu. Go to the online Help to learn more about these important functions.
- Add interfaces to the selected agent by right-clicking the content area of the view and selecting Add Interface.
- Start a remote session (in which you can run an agent troubleshooting application on the specific interface) by right-clicking a highlighted interface listing and clicking the Open Remote Session menu option. See page 57 for more details.
- Set custom data thresholds for a specific interface by using the right-click menu.
- Configure interface-specific alarms by using the right-click menu.
- Perform other interface-specific functions such as configuring collections on a VLAN or PVC, or running a WAN Latency measurement, or others.

Another aspect of agent management is SNMP Mapping. SNMP mapping sets the auto-discovery, auto-collection, and agent type/class policies that will be applied when an agent is contacted during SNMP discovery. NTC's default agent mappings account for a large number of common agent types.

Right-click an SNMP map listing or anywhere in the content area to add, delete, enable, disable, or modify an SNMP mapping.

Each table row shows important information about the association between the ObjectID, MIB, and agent class, and description.


Agilent Network Troubleshooting Center - Agilent NTC Test
Address Agent Manager/SNMP Mapping
Agent Manager
Agents
SNMP Discovery
SNMP Mapping
Real-Time Collections
Health Summary
Event Viewer
Global Configuration
Help
Agents | SNMP Discovery | SNMP Mapp
User | SysObjectID | MIB | Class | Collection | Discovery | Description
No | 1.3.6.1.4.1.11.2.3.7.11.1 | switch | Disabled | Enabled | HP Switch 2000A (J3100A)
No | 1.3.6.1.4.1.11.2.3.7.11.10 | switch | Disabled | Enabled | HP Switch 2400T (J4122A)
No | 1.3.6.1.4.1.11.2.3.7.11.2 | switch | Disabled | Enabled | HP Switch 2000B (J3100B)
No | 1.3.6.1.4.1.11.2.3.7.11.3 | switch | Disabled | Enabled | HP Switch 800T (J3245A)
No | 1.3.6.1.4.1.11.2.3.7.11.4 | switch | Disabled | Enabled | HP Switch 208 and 224 (J3175A, J3177A)
No | 1.3.6.1.4.1.11.2.3.7.11.5 | switch | Disabled | Enabled | HP Switch 212M (J3298A)
No | 1.3.6.1.4.1.11.2.3.7.11.6 | switch | Disabled | Enabled | HP Switch 224M (J3299A)
No | 1.3.6.1.4.1.11.2.3.7.11.7 | switch | Disabled | Enabled | HP Switch 8000 (J4110A)
No | 1.3.6.1.4.1.11.2.3.7.11.8 | switch | Disabled | Enabled | HP Switch 1600 (J4120A)
No | 1.3.6.1.4.1.11.2.3.7.11.9 | switch | Disabled | Enabled | HP Switch 4000 (J4121A)
No | 1.3.6.1.4.1.11.2.3.7.5.20 | Hub | Disabled | Enabled | HP Hub12M (J3301A)
No | 1.3.6.1.4.1.11.2.3.7.5.21 | Hub | Disabled | Enabled | HP Hub12M (J3303A)
No | 1.3.6.1.4.1.11.2.3.7.6.10.2.1 | lan | Enabled | Enabled | HP Multiport Ethernet LanProbe (J3912A)
No | 1.3.6.1.4.1.11.2.3.7.6.11.1.1 | wan | Enabled | Enabled | HP T1 WANProbe with Ethernet Telemetry (J3913A)
No | 1.3.6.1.4.1.11.2.3.7.6.12.1.1 | wan | Enabled | Enabled | HP E1 WANProbe with Ethernet Telemetry (J3914A)
No | 1.3.6.1.4.1.11.2.3.7.6.13.1.1 | wan | Enabled | Enabled | HP V-Series WANProbe with Ethernet Telemetry (J3915A)
No | 1.3.6.1.4.1.11.2.3.7.6.14.1.1 | wan | Enabled | Enabled | HP HSSI WANProbe with Ethernet Telemetry (J3916A)
No | 1.3.6.1.4.1.11.2.3.7.6.15.1.1 | wan | Enabled | Enabled | HP T3/DS-3 WANProbe with Ethernet Telmetry (J3917A)
No | 1.3.6.1.4.1.11.2.3.7.6.16.1.1 | wan | Enabled | Enabled | HP UTP ATMProbe with Ethernet Telemetry (J3918A)
No | 1.3.6.1.4.1.11.2.3.7.6.17.1.1 | wan | Enabled | Enabled | HP OC-3 ATMProbe with Ethernet Telemetry (J3919A)
No | 1.3.6.1.4.1.11.2.3.7.6.18.1.1 | wan | Enabled | Enabled | HP DS-3 ATMProbe with Ethernet Telemetry (J3920A)
No | 1.3.6.1.4.1.11.2.3.7.6.19.1.1 | wan | Enabled | Enabled | HP E3 ATMProbe with Ethernet Telemetry (J3921A)
No | 1.3.6.1.4.1.11.2.3.7.6.21.1.1 | lan | Enabled | Enabled | HP Gigabit Ethernet LanProbe
No | 1.3.6.1.4.1.11.2.3.7.6.3 | lan | Enabled | Enabled | HP LanProbe II
No | 1.3.6.1.4.1.11.2.3.7.6.3.1 | lan | Enabled | Enabled | HP LanProbe II
No | 1.3.6.1.4.1.11.2.3.7.6.3.2 | lan | Enabled | Enabled | HP LanProbe II
No | 1.3.6.1.4.1.11.2.3.7.6.3.3 | lan | Enable | Enabled | HP LanProbe III (4986A/4987A) and HP Ethernet LanProbe (
No | 1.3.6.1.4.1.11.2.3.7.6.6 | lan | Disable | Enabled | NetMetrix probe
No | 1.3.6.1.4.1.11.2.3.7.6.7.2.1 | lan | Enable | Enabl | HP Quad Ethernet LanProbe (J3457A)
No | 1.3.6.1.4.1.11.2.3.7.6.9.1.1 | lan | Enable | Enabled | HP Fast Ethernet LanProbe (J3458A)
Help
Agent Mapping tab - Use this tab to specify the type of agents that NTC can discover and add during SNMP discovery. Right-click to add, modify, or delete an agent mapping.
Help

Each table row also shows the auto-collection and auto-discovery policy that will be applied when an agent of the specified type is discovered.

Viewing Collected MIB-II, RMON, and RMON2 Data

Once you have added or discovered agents, and performed any agent management tasks to make sure they are gathering data, you can view that data in a number of ways. You can:

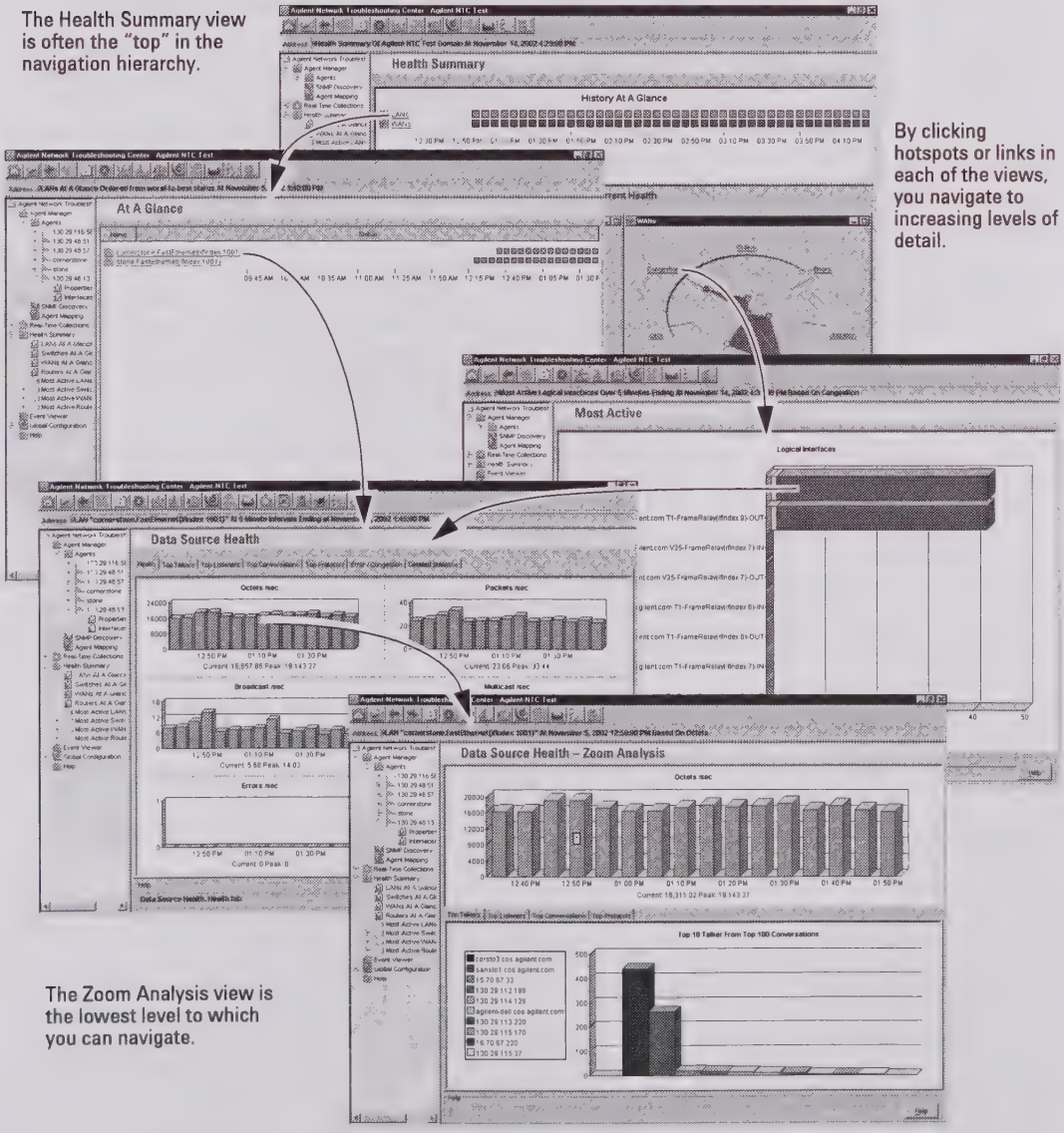
- Open specific data views from the Navigation tree.
- Open Data Source Health views for specific data sources from the Agent Interfaces view.
- Open the Health Summary view and navigate into the data and to a specific data source.

This last option is described in the following pages.

The following diagram shows how you can navigate through NTC's data views to look at collected SNMP/RMON2 data.

The Health Summary view is often the "top" in the navigation hierarchy.

By clicking hotspots or links in each of the views, you navigate to increasing levels of detail.



The Zoom Analysis view is the lowest level to which you can navigate.

Note the following with regard to viewing SNMP/RMON2 data:

- Data collection must be started on agent interfaces and at least 2 collection intervals will pass before data begins appearing in the data display views.
- The Health Summary, At A Glance, and Most Active views are "summary" views that show data aggregated from several sources. The Data Source Health and Zoom Analysis views display data from single data sources.
- As you navigate through data, your progress is tracked in the Navigation tree. You can use the back button to go back to views previously seen.
- In most cases, data is displayed using red, yellow, and green colors. Red and yellow indicate critical and warning thresholds have been exceeded. Thresholds are set in the Threshold tab in Global Configuration. See the online Help for more information.
- In the Data Source Health view, you can perform both historical and real-time data collection. Refer to the Help for details.
- You can open a remote session window and run Network Analyzer software on a specific agent interface from the Data Source Health view and from the Zoom Analysis view. Troubleshooting using a remote session window is described in the next section.
- SNMP/RMON2 data collection is done using Network Analyzer and Distributed Network Analyzer agents on Ethernet interfaces only.

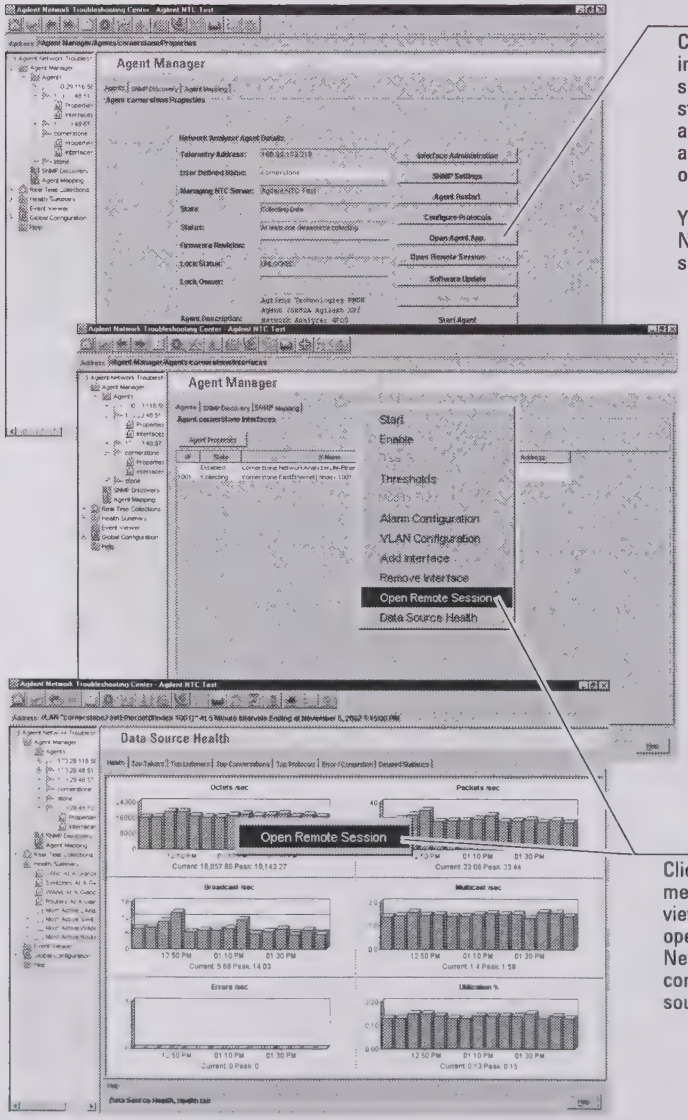
Running a Remote Troubleshooting Session on an Agilent Agent

NTC provides access, via a remote session window, to Network Analyzer software running on a Distributed Network Analyzer MX, a Distributed Network Analyzer ME, a Network Analyzer dispatched tester, or an appropriately configured and equipped PC.

A remote session is a way for a remotely located NTC Console to log into a Network Analyzer or Distributed Network Analyzer agent and run the resident network test software on that agent.

Running this type of remote troubleshooting session is often a follow-up step to the problem isolation process that uses NTC's SNMP/RMON2 data collection. However, there are many cases where it makes sense to go directly to the remote troubleshooting session on a supported Network Analyzer test platform using NTC as a launch point.

This diagram shows three of the points from which a remote troubleshooting session can be started.



Click the Open Remote Session button in Agent Properties to open a remote session window to the agent without starting the Network Analyzer application. (You can start the application once the remote window is open.)

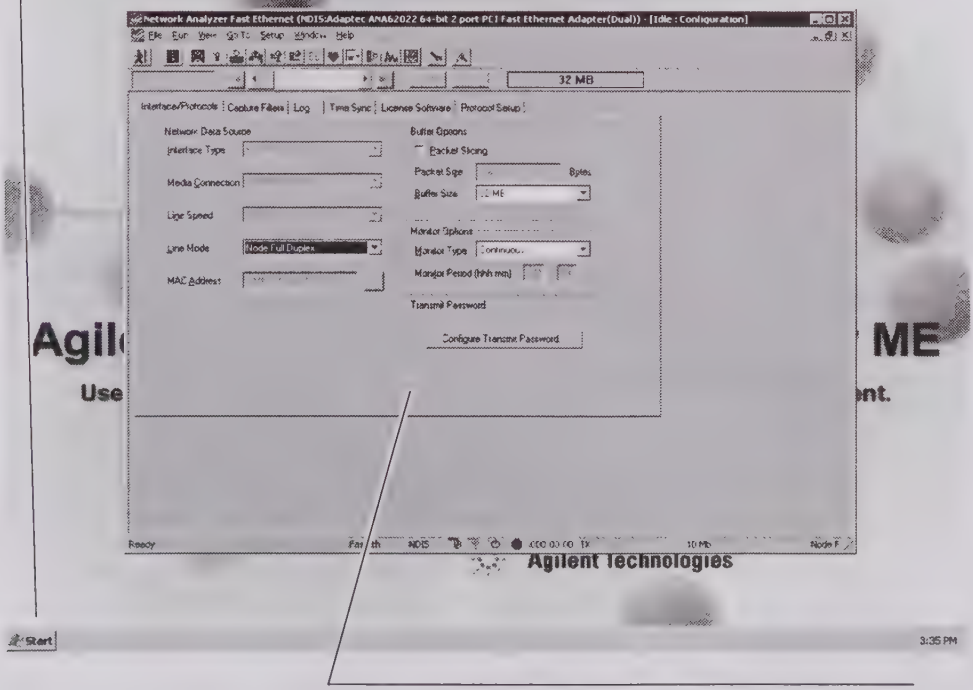
You can also right-click an agent in the Navigation tree to open the remote session window.

To the remote session window.

Click the Open Remote Session right-click menu option in either the Agent Interfaces view or the Data Source Health view. This opens the remote session window with the Network Analyzer software started and configured for the selected interface / data source.

The remote session window allows you to run Network Analyzer software on the Network Analyzer dispatched tester, Distributed Network Analyzer MX/ME, or appropriately configured and equipped PC.

If it is not already started due to the method you used to access the remote session window, you can start the Network Analyzer software using the remote session window Start menu.



Once started, you can operate the Network Analyzer Software as if you were sitting at a keyboard and monitor at the device itself. You can go back to NTC by closing the remote session window, and leave the Network Analyzer running if you want.

Refer to NTC's online Help for more operational details.

Other Useful Features to Note

Strictly speaking, it is not necessary to use the features mentioned in this section as part of the "getting started" process. However, you might want to alter some aspect of the configurations to better suit your testing and monitoring situation.

Event Viewer

The Event Viewer is, by default, configured to display events related to the following:

- Exceeded thresholds
- RMON alarms
- Changes to data collection status
- Unreachable data sources

You might want to filter which events are visible in the viewer or configure traps to be sent to other network test applications and systems. Refer to the online Help for more detailed information.

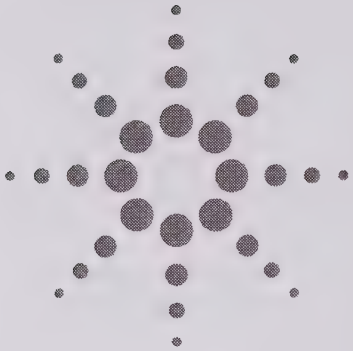
Global Configuration

Global Configuration concerns itself with globally applied monitor thresholds, security, data storage, and others. By default, these configurations are set to reasonable values and need not be changed initially. However, because of your test and monitor needs, you might want to change a number of settings, the most likely of which include thresholds, data storage, and security. Refer to the online Help for more information.

NTC Console Customization

You can make some common changes to the NTC Console. These changes are not considered part of Global Configuration and will only apply to your workstation. To customize your Console, you can:

- Change display preferences to identify hosts by their friendly name or by their network IP address.
- Change the time-frame for historical data display.



3
Licensing, Performance, and Other Operational Information

Licensing 64
Integrating with HP OpenView Network Node Manager 69

Licensing

For every licensed copy of the Network Troubleshooting Center (NTC), you can:

- Install the NTC Console on any number of computers limited only by the processing power of the computer on which the managing NTC Server is installed.
- Install one NTC Server on a single computer.
- Collect SNMP/RMON2 data on a fixed number of physical interfaces simultaneously. The number of allowed physical interfaces is determined by the product you receive.

The number of physical interface licenses you have is determined by the option you purchased.

Please note the following information with regard to NTC licensing and operation:

Purchasing an NTC Product Allowing More Physical Interfaces

Every Network Analyzer product purchase receives a 4-physical interface license as part of the product. Therefore, with every Network Analyzer purchase, you can install NTC and collect SNMP/RMON2 data from 4 physical interfaces simultaneously.

If you want to be able to collect data from more interfaces simultaneously, you must purchase another NTC product specifying a particular option. Note, however, that this is not necessarily an upgrade. For example, if you purchase the 10-interface license (and already have the 4-interface license, you can:

- Install the 10-interface license on the same computers as the 4-interface license. In this case, you will still have only *one* NTC Server and be allowed to collect data on 10 interfaces simultaneously.

- Install the 10-interface license on a different set of computers than the 4-interface license. In this case, you will have *one* NTC Server capable of managing collections on 4 physical interfaces simultaneouslyand have *another* NTC Server capable of managing 10 physical interfaces simultaneously.

Remember, for either of the examples above, the number of NTC Console installations is not affected. Each Console can log in to any Server. How you choose to deploy multiple product purchases depends on your test situation.

Data Sources, Logical Interfaces, and Physical Interfaces

In the context of NTC, there is a difference between distinct data collections, data sources, logical interfaces, and physical interfaces. In general, the term "interface" can mean several different things in NTC depending on the context. Please note the following definitions with regard to these differences.

- **Physical Interface**
  Also sometimes called a port, this term corresponds to a physically distinct interface. Physical interfaces are also known in NTC as "Agent Interfaces" are presented in the view/window with the same name. A physical interface may contain one or more logical interfaces.
- **Logical Interface**
  Also known as a virtual interface, a logical interface is typically a logical subdivision of physical port traffic. Multiple logical interfaces may be contained within the same physical interface or port. Examples include WAN PVCs, and VLANs on an 802.1Q switch link.
- **Data Source**
  This is a physical or logical entity that provides a uniquely identifiable set of scalar measurement statistics that are available for data collection. A data source can be associated with a physical or logical interface. Each measurement on an interface is a different data source.

- **Data Collection**
  A data collection is a distinct set of SNMP measurements. There are two types: historical and real-time. It is possible to one historical data collection and one real-time data collection on a single data source. Historical and real-time data collections are discussed below and in the NTC online Help.

The next section puts into context the concepts of physical interfaces, data sources, and performance requirements.

Licensing and Performance Requirements

It is important to note that an NTC license is concerned only with simultaneous collections on physical interfaces. However, the number of data collections can have an impact on the performance of NTC and on the number of agents (and therefore physical interfaces) you plan to add and collect data from. That is, when the number of data collections is increased, CPU and Memory requirements can increase as well. Listed below are additional performance requirements in the context of increased numbers of data collections.

These requirements apply to a single NTC Server-only installation. The NTC Console installation and operational requirements are not affected by higher numbers of data collections. These requirements also assume standard hardware and software configurations (cache, memory speed, etc.), that only the NTC Server is running, and that minimum installation requirements (as described in the Hardware Setup Guides) are met.

Historical Collections (5 minute collection interval)

Supports Up To 25 Historical Collections

- Minimum CPU Speed: 500 Mhz
- Minimum Memory (RAM): 256 Mbytes

Supports Up To 120 Historical Collections

- Minimum CPU Speed: 700 Mhz
- Minimum Memory (RAM): 256 Mbytes

Supports Up To 150 Historical Collections

- Minimum CPU Speed: 1 Ghz
- Minimum Memory (RAM): 256 Mbytes

Supports Up To 200 Historical Collections

- Minimum CPU Speed: 2 Ghz
- Minimum Memory (RAM): 500 Mbytes

Supports Up To 400 Historical Collections

- Minimum CPU Speed: 2 Ghz
- Minimum Memory (RAM): 1 Gbytes

Real-time Collections (10 second collection interval)

Co-existing with 100 historical collections on the same NTC Server.

Supports Up To 1 Real-time Collections

- Minimum CPU Speed: 500 Mhz
- Minimum Memory (RAM): 256 Mbytes

Supports Up To 10 Real-time Collections

- Minimum CPU Speed: 700 Mhz
- Minimum Memory (RAM): 256 Mbytes

Supports Up To 15 Real-time Collections

- Minimum CPU Speed: 2 Ghz
- Minimum Memory (RAM): 500 Mbytes

Supports Up To 20 Real-time Collections

- Minimum CPU Speed: 2 Ghz
- Minimum Memory (RAM): 1 Gbyte

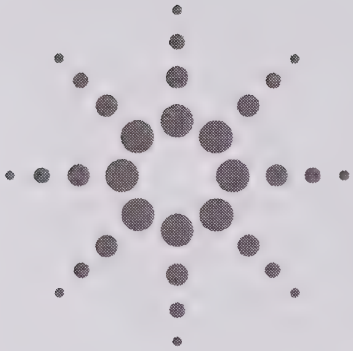
Licensed Physical Interfaces and Starting a Remote Session

The number of physical interfaces allowed by a particular NTC license has no effect on the number of remote session window you can open to a particular agent. In other words, even if you are licensed for data collection on 4 physical interfaces, you can

start more than 4 remote session windows. This number is limited only by the processing power of the computer on which the NTC Console is installed, management network performance, and the agent on which the remote session window is run.

Integrating with HP OpenView Network Node Manager

If you have HP OpenView Network Node Manager installed and you want to forward captured events to that program for further analysis, you must load an NTC MIB definition (provided with the NTC installation) into the HP product. The instructions to perform the load are not included in this document because you perform the load using the HP OpenView Network Node Manager product. Please see the Event Policy topics in the NTC online Help for more information.



A Appendix: RMON/RMON2 Fundamentals

Managing Networks Using RMON Data 72

Using NTC to Monitor RMON Data Collection 75

Allocating Memory for the RMON Table 79

Managing Networks Using RMON Data

This appendix provides a basic level of information about RMON data collection on the Network Analyzer products. The Network Troubleshooting Center (NTC) 1.0 release with the Network Analyzer Software 2.0 release support Remote Monitoring (RMON) data collecting in conjunction with SNMPv1.

SNMP Version 1 (SNMPv1) is the current standard version of the SNMP protocol, which is an IETF standard defined in RFC 1157. RMON is an extension to the basic SNMP standard that provides the ability to manage LANs as well as devices attached to those networks.

RMON Version 1 (RMON) is defined in RFC 2819; and its enhanced version, RMON Version 2 (RMON/2), is defined in RFC 2021. Another standard, MIB-II, provides general TCP/IP management information.

These specifications that define SNMP, RMON, and MIB-II can be found at the Internet Engineering Task Force located at www.ietf.org.

Overview of SNMP, MIB-II, and RMON

The SNMP protocol is an application-layer protocol standard for managing TCP/IP based networks. SNMP provides a set of operations that allows devices on your network to be managed remotely. The SNMP protocol allows you to monitor your network constantly. It examines packets coming through your network and notifies you if a potential problem exists.

The SNMP protocol is also considered a network management system that contains management stations and SNMP-capable devices. A network management station is a PC or workstation running a software system that can handle management tasks for a network. Network Management Stations are commonly referred to as NMSs. An NMS polls and receives SNMP data traps from agents in a network.

A poll involves the act of querying an agent for some piece of information. The agent is a piece of software that runs on the network devices you are managing. When the agent notices that something is causing a problem on your network, it can send a trap to the NMS. A trap is the way an agent informs the NMS that an event has occurred. A trap is an asynchronous notification sent from an SNMP agent to a network management station. A trap represents a collection of data defined by a managed object.

SNMP sends and receives information by using the User Datagram Protocol (UDP), which is defined in RFC 768. This means that no end-to-end connection is made between the agent and the NMS when datagrams (packets) are sent back and forth. UDP runs over the IP layer to deliver the packet. UDP allows the NMS and agent to communicate with one another. The IP layer delivers the SNMP packet to its destination, where it is handed off to the physical network.

Each SNMP packet contains a community string for security purposes. The community string in the SNMP statement must be the same as the one in the SNMP agent so communication between the NMS and agent can occur.

A brief overview about Management Information Base objects follows before discussing the SNMP/RMON2 data collection that NTC manages on the Agilent Network Analyzer products.

Management Information Base (MIB)

The Management Information Base (MIB) is a database of managed objects that an agent tracks and is accessed by the NMS. A MIB contains a definition of the managed object and explains its meaning. In other words, the objects in the MIB are used as object identifiers, which means a textual string is used as a descriptor.

The particular MIB standard that is implemented by all SNMP agents is MIB-II. MIB-II provides general TCP/IP management information.

The implementation of RMON data collections for this software release includes RMON MIBs, MIB-II, and Agilent private MIBs. The Agilent private MIBs are not included in this Appendix.

RMON MIB

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

RMON is a supplement to the MIB-II group. RMON delivers information in nine RMON groups of monitoring elements, each providing a specific set of data to meet common network requirements. RMON provides the NMS with MAC-level statistics.

RMON/2 adds an additional capability by providing network and application-level statistics. RMON/2 delivers information in nine RMON groups of monitoring elements.

See RFC 2021 and RFC2074, *Remote Network Monitoring Management Information Base Version 2*, for more information. See RFC1213, *Management Information Base for Network Management of TCP/IP-based internets: MIB-II*, for more information about these groups.

Using NTC to Monitor RMON Data Collection

SNMP, RMON, and RMON2 (SNMP/RMON2) are remote networking monitoring standards that enable various network monitors and console systems to exchange networking monitoring data. The implementation of SNMP/RMON2 capability for the Network Analyzer devices is available when a 10/100/1000 Ethernet LIM is installed in the following Agilent Network Analyzer products:

- J6800A Network Analyzer
- J6801A Distributed Network Analyzer
- J6802A Distributed Network Analyzer MX

The 10/100 NDIS NIC interfaces on the J6805A Distributed Network Analyzer ME have SNMP/RMON2 capability enabled.

As part of the Network Analyzer Solutions, NTC is used to monitor SNMP/RMON2 data collection on the Network Analyzer products. The RMON agent software that resides on the Network Analyzers is responsible for the collection of SNMP/RMON2 data.

RMON and MIB-II Supported Groups

Agilent supports specific groups in the RMON, RMON/2, and MIB-II protocols. NTC utilizes a subset of this information as listed below:

- Agilent supports four of the nine groups of the RMON MIB: Ethernet Statistics, Alarm, History, and Event.
- Agilent supports all nine groups for the RMON/2 MIB.
- NTC uses the data from four of the RMON/2 MIB groups: Protocol Directory, Network Layer Host, Application Layer Host, and Probe Configuration.
- Agilent supports three of the nine groups in MIB-II: System, Interfaces, and SNMP.

Accessing RMON Data through NTC

NTC coordinates the data collection methods for the SNMP/RMON2 measurements. The default startup mode on the DNA MX and DNA ME is SNMP/RMON2 mode. For the J6800A Network Analyzer and PC agent connected to a J6801A, you must start the agent services manually by using the NTC Agent Services.

The RMON agent gathers statistical information from a subset of these RMONv2 and MIB-II groups and reports the data collection to NTC. NTC monitors the status of a Network Analyzer from the RMON data collection.

The RMON agent notifies NTC through standard traps. A trap is a collection of data that is defined by a particular MIB. A few of the trap formats and contents are described next.

- ColdStart – The RMON agent has performed a cold start and factory defaults have been restored.
- WarmStart – The RMON agent has performed a warm start, all control tables are still persistent, and data tables are cleared.
- LinkDown – An interface has gone down due to the link being disconnected.
- LinkUp – An interface has become active due to a link being restored.

Other proprietary traps exist for interface status. Contact Agilent Technical Support for more information.

The LinkDown and LinkUp traps are particularly important in understanding how NTC monitors the Network Analyzer and SNMP/RMON2 applications that run on the Network Analyzer devices. This scenario, described next, occurs when a user wants to start the Network Analyzer application on a Network Analyzer device while the SNMP/RMON2 application is running.

NTC communicates to the Network Analyzer device about switching the application from SNMP/RMON2 mode to the Network Analyzer mode. The Network Analyzer stops the

SNMP/RMON2 data collection on its acquisition systems and moves the interface to status down, while it is troubleshooting in Network Analyzer mode.

When the user exits from the Network Analyzer application, NTC communicates to the Network Analyzer device to stop the application. The device stops the Network Analyzer data collection and moves the interface to status up to start the SNMP/RMON2 data collection again.

For the Distributed Network Analyzer MX upon exiting the Network Analyzer application, the acquisition system reboots, which means a ColdStart Trap is sent when the interface changes. For the Distributed Network Analyzer ME, a WarmStart Trap is sent to indicate the DNA ME is back in SNMP/RMON2 mode. For the J6800A Network Analyzer and PC agent, you must manually reset the device to SNMP/RMON2 mode.

Accessing RMON Data by Non-NTC Systems

The SNMP protocol utilizes community strings to establish trust between managers and agents. Non-NTC systems, like HP OpenView and others, are allowed to access the SNMP/RMON2 data information gathered on the Agilent Network Analyzers.

These non-NTC systems are considered third-party applications or NMSs that may need to gather statistics from Agilent devices.

The SNMP/RMON2 agent in the J6800A Network Analyzer, J6801A Distributed Network Analyzer, J6802A Distributed Network Analyzer MX, and the J6805A Distributed Network Analyzer ME support the following community strings and access levels as described in the next table:

Community String	Level
Public	1
RMON	2
RMON_admin	3
agilent_admin	4
at_admin	4

Allocating Memory for the RMON Table

The memory allocated for all RMON tables is 64 MBytes of system RAM. Here is a list of the table groups that are configured on the RMON agent probe and their maximum sizes.

Table Name	Maximum Entries
Host Table Size	180000
Maximum Number of RMON MIB TopN Studies	Unlimited
Maximum Entries per TopN Studies	220000
Maximum Traffic Matrix Table Size	250000
Maximum Number of RMON MIB History Studies	Unlimited
Total Number of History Buckets	750000
Network Layer Host Table Size	220000
Network Layer Traffice Matrix Table Size	180000
Application Layer Host Table Size	220000
Application Layer Traffic Matrix Table Size	180000
Maximum Entries Per RMON2 TopN Study	120000
Maximum Entries Per RMON2 Address Map	780000
Maximum Number of Alarms	50000
Maximum Number of Events	120000
Log Table Entries	380000
Maximum Number of Filters	N/A
Maximum Number of Channels	N/A
Maximum Number of Capture Buffers	N/A
Trace Buffer Packet Capacity	N/A
Trace Buffer Octet Capacity	N/A

Maximum Number of Community Names in Com Access Table	Unlimited
Maximum Number of Trap Destinations	Unlimited
Maximum SLIP Connection Entries	N/A
MaximumSingle Shot Pings	N/A
Maximum List Pings	N/A

B
Appendix: Copyright Notices

Copyright Notices and Acknowledgements

The Network Troubleshooting Center uses a number of third-part components. The copyright acknowledgements for these components are included in this appendix.

Copyright © 2002 Agilent Technologies, Inc. All Rights Reserved.

Copyright © 1985-2002 Microsoft Corporation. All rights reserved.

Copyright © 1994-2002 Sun Microsystems, Inc. All rights reserved.

Copyright © 2000 by NETAPHOR SOFTWARE, INC.

ACE(TM) and TAO(TM) are copyrighted by Douglas C. Schmidt and his research group at Washington University and University of California, Irvine, Copyright © 1993-2001, all rights reserved.

SOLID logo with the text "SOLID" is a registered trademark of Solid Information Technology Ltd. SOLID Embedded Engine ™ and SOLID DBConsole ™ are trademarks of Solid Information Technology Ltd. –

Copyright © 1992-2000 Solid Information Technology.

Copyright © 1997-2001 by Gerald Brose.

Copyright © 1996-2000 SITRAKA INC. All Rights Reserved.

Copyright © 1998 John E. Bossom

Copyright © 1999,2002 Pthreads-win32 contributors

Copyright © 1988-1997 Epilogue Technology Corporation.

Copyright © 1998 Integrated Systems, Inc. All Rights Reserved.

Copyright © 1993 - 2000 by Apptitude, Inc, San Jose, CA, U.S.A. All Rights Reserved.

Copyright © 1999-2002, Politecnico di Torino. All rights reserved.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

The Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
"This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ‘ ‘ AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* ====================

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Index

A

adding agents, 43
Agent Interfaces, 19, 48, 51, 58
Agent Manager, 43
Agent Properties, 19, 48, 49, 58
agents, 11, 13, 42
  agent application, 20
  Agent Interfaces, 51
  agent management, 19
  Agent Properties, 49
  auto-discovery, 19
  deploying, 29
  discovering, 45
  general SNMP agents, 14, 32
  managing, 47
  manually adding, 43
  Network Analyzer, 14, 29
Agents tab, 43
alarms, 10, 25
architecture, 11
At A Glance view, 22, 55

C

capabilities, 10, 18
collection intervals, 66
collections, 65
community string, 44
components, 11
configurations, 26, 60
console, 11
copyright notices, 72
critical thresholds, 56
customizing the NTC Console, 60

D

data collection, 12, 20, 50, 54, 65
  historical vs. real-time, 65
  performance considerations, 66
  real-time, 56
data display, 20, 54
Data Source Health view, 22, 55, 58
data sources, 65
data storage, 26
database, 35, 38
deploying agents, 29
deploying NTC, 15
detailed troubleshooting, 12, 20, 24, 57
discovering agents, 45
Distributed Network Analyzer
  as an agent, 14
DNA MX/ME, 10, 14, 29

E

errors, 25
event policy, 26
Event Viewer, 25, 60

F

features, 10, 18

G

Global Configuration, 26, 60
Greenwich Mean Time (GMT), 31

H

hardware
  setting up, 29
Health Summary view, 22, 55
historical collections, 65
historical data, 10
HP OpenView, 68

I

installing NTC, 34
interfaces, 17, 50, 51
  licensing, 64
  physical vs. logical, 65
Introduction, 10
IP addresses, 35, 40, 45

L

licensing, 17, 34, 38, 39, 64, 67
  performance considerations, 66
  remote session, 67
localhost, 40
logging in to the server, 40

M

managing agents, 47
mapping
  SNMP agents, 19
message size, 44
MIB-II, 10, 20, 54
mode switch, 57
monitor results, 54
Most Active view, 22, 55
multi-homed host, 40

N

NetMetrix Probes, 14
Network Analyzer, 10, 56, 57, 59
  as an agent, 14, 29
  measurements, 12
  used with NTC, 24
network diagram, 15
network management stations, 36
Network Troubleshooting Center (see NTC), 10
NMS, 36, 68

NTC
  accesses Network Analyzer, 24
  components of, 11
  deploying agents, 29
  deployment diagram, 15
  installing, 34
  Introduction, 10
  licensing, 34, 38
  setting up, 28
  starting, 37
NTC Console, 13, 17, 34, 39, 60
NTC Server, 13, 17, 34, 35, 36, 37
  logging in, 40

O

opening a remote session window, 50, 52, 56, 57
Overview
  features, 18
  setup process, 28

P

PC
  as an agent, 14, 30
performance, 66
port number, 44
problem isolation, 10
Properties, 49
PVC, 52

Q

Quick Start Navigator, 41

R

real-time collections, 65
real-time data, 10
real-time data collection, 56
remote session window, 10, 12, 20, 24, 50, 52, 56, 57, 67
RMON, 10, 12, 20
RMON/RMON2, 54
RMON2, 10, 12, 20

S

saving the database, 35
security, 26
seed address, 45
server, 11, 26
setting up, 15, 29
setup process, 28
SNMP, 10, 12, 20, 32, 44
SNMP Discovery, 19, 45
SNMP Mapping, 19, 46, 53
software
  installing, 29, 34
starting NTC, 37
storage, 26

T

thresholds, 26
time zone settings, 31
traps, 10
troubleshooting
  using a remote session window, 57

V

violations, 25
VLAN, 52

W

WAN Latency, 52
warning thresholds, 56
warnings, 25

Z

Zoom Analysis view, 22, 55

www.agilent.com

Together with Agilent, gain the eXtreme Productivity Improvements that your business demands!

www.agilent.com/comms/XPI

Product specifications and descriptions in this document subject to change without notice.

© Agilent Technologies, Inc. 2002-2003

Printed in Singapore January 2003

5971-6321

Agilent Technologies